CYBER RISK INSTITUTE

The CRI Profile Guidebook

Guidance for Implementing the CRI Profile ver. 2.2 and Responding to its Diagnostic Statements

April 2026

Cyber Risk Institute
Washington, D.C.

CyberRiskInstitute.org

The CRI Profile is the result of tremendous effort from many organizations of varying sizes and complexities. We want to extend our gratitude to the financial institutions, regulatory groups, and other organizations who contributed to this initiative. We want to particularly thank BCG Platinion, which provided initial support to the Profile's development, and EY which provided expertise and manpower to this important sector initiative. We also want to thank our 100+ member organizations, our CRI Board of Directors, which provided the strategic guidance, and the CRI Profile Architecture Working Group, which reviewed and validated all of the Profile's content and mappings. Finally, we want to acknowledge CRI's John Goodman and Emily Beam for their tireless thought leadership, contract oversight, and member engagement.

We continue to thank Ann Lavis, Heidi Erchinger, and Kevin Isabelle from HSBC who developed the first comprehensive draft of the Profile Guidebook, as well as Stephanie Wake and Kevin Gronberg, who performed the first extensive review. Their work is of tremendous ongoing benefit to the Profile and the sector overall.

-The CRI Team

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. *To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.*

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. *To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.*

CYBER RISK INSTITUTE

TABLE OF CONTENTS

CRI PROFILE VER. 2.2 GUIDEBOOK CHANGE LOG 6

ABOUT THE CRI PROFILE GUIDEBOOK 7

- Background 7
- Purpose 7
- Intended Audience 7
- Contents 8

GETTING STARTED 11

- Determine Your Organization's Impact Tier 11
- Assess Your Organization's Cyber Risk Management Program Using the Profile's Diagnostic Statements 11
- Response Key 12
- Tips for Completing the Profile and for Use with the Examination Staff 12

DIAGNOSTIC STATEMENT REFERENCE 14

- GOVERN / Organizational Context / Organizational Mission 14
- GOVERN / Organizational Context / Stakeholder Risk Management Expectations 15
- GOVERN / Organizational Context / Legal, Regulatory, & Contractual Requirements 21
- GOVERN / Organizational Context / Stakeholder Service Expectations 24
- GOVERN / Organizational Context / Organizational Service Dependencies 32
- GOVERN / Risk Management Strategy / Risk Management Objectives Agreement 42
- GOVERN / Risk Management Strategy / Risk Appetite & Risk Tolerance Statements 55
- GOVERN / Risk Management Strategy / Enterprise Risk Integration 60
- GOVERN / Risk Management Strategy / Risk Response Strategic Direction 69
- GOVERN / Risk Management Strategy / Lines of Communication 71
- GOVERN / Risk Management Strategy / Standardized Risk Management Method 76
- GOVERN / Risk Management Strategy / Strategic Opportunities 78
- GOVERN / Risk Management Strategy / Technology Assimilation & Implementations 80
- GOVERN / Risk Management Strategy / Business Continuity & Resilience Risk Management 92
- GOVERN / Roles, Responsibilities, and Authorities / Organizational Leadership Responsibility 99
- GOVERN / Roles, Responsibilities, and Authorities / Risk Management Roles & Responsibilities 109
- GOVERN / Roles, Responsibilities, and Authorities / Resource Adequacy 118
- GOVERN / Roles, Responsibilities, and Authorities / Human Resource Practices 122
- GOVERN / Policies, Processes, and Procedures / Establishment of Policies & Procedures 127
- GOVERN / Policies, Processes, and Procedures / Policy & Procedure Review & Update 137
- GOVERN / Oversight / Risk Management Strategy Outcomes Review 138
- GOVERN / Oversight / Risk Management Strategy Review & Adjustment 142
- GOVERN / Oversight / Risk Management Performance Measurement 145
- GOVERN / Supply Chain Risk Management / Supply Chain Risk Management Program 147
- GOVERN / Supply Chain Risk Management / Third Party Roles & Responsibilities 150
- GOVERN / Supply Chain Risk Management / Supply Chain Risk Management Integration 151
- GOVERN / Supply Chain Risk Management / Supplier Identification & Prioritization 152
- GOVERN / Supply Chain Risk Management / Third Party Incident Management Integration 153
- GOVERN / Supply Chain Risk Management / Supply Chain Security Practice Integration 154
- GOVERN / Independent Risk Management Function / Independent Risk Management Function 155
- GOVERN / Independent Risk Management Function / Independent Risk Management Evaluation 158
- GOVERN / Independent Risk Management Function / Independent Risk Management Reporting 160
- GOVERN / Independent Audit Function / Independent Audit Compliance Assessment 161
- GOVERN / Independent Audit Function / Independent Audit Procedures 166
- GOVERN / Independent Audit Function / Independent Audit Reporting 168
- IDENTIFY / Asset Management / Hardware Inventory 170

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

IDENTIFY / ASSET MANAGEMENT / SOFTWARE, SERVICES, & SYSTEMS INVENTORY 172
IDENTIFY / ASSET MANAGEMENT / NETWORK COMMUNICATIONS & DATA FLOWS 173
IDENTIFY / ASSET MANAGEMENT / SUPPLIER SERVICES INVENTORY 174
IDENTIFY / ASSET MANAGEMENT / ASSET PROTECTION PRIORITIZATION 176
IDENTIFY / ASSET MANAGEMENT / DATA & METADATA INVENTORY 179
IDENTIFY / ASSET MANAGEMENT / ASSET LIFE CYCLE MANAGEMENT 180
IDENTIFY / ASSET MANAGEMENT / ASSET LIFE CYCLE MANAGEMENT 183
IDENTIFY / RISK ASSESSMENT / ASSET VULNERABILITY IDENTIFICATION 187
IDENTIFY / RISK ASSESSMENT / INFORMATION SHARING FORUMS 190
IDENTIFY / RISK ASSESSMENT / THREAT IDENTIFICATION 193
IDENTIFY / RISK ASSESSMENT / IMPACT & LIKELIHOOD ANALYSIS 197
IDENTIFY / RISK ASSESSMENT / RISK EXPOSURE DETERMINATION & PRIORITIZATION 197
IDENTIFY / RISK ASSESSMENT / RISK RESPONSE DETERMINATION 201
IDENTIFY / RISK ASSESSMENT / CHANGE & EXCEPTION MANAGEMENT 208
IDENTIFY / RISK ASSESSMENT / VULNERABILITY DISCLOSURE RESPONSE 214
IDENTIFY / IMPROVEMENT / CONTINUOUS IMPROVEMENTS EVALUATION 217
IDENTIFY / IMPROVEMENT / TESTS & EXERCISES 221
IDENTIFY / IMPROVEMENT / IMPROVEMENTS FROM LESSONS LEARNED 234
IDENTIFY / IMPROVEMENT / PLANS AFFECTING OPERATIONS 235
PROTECT / IDENTITY MANAGEMENT, AUTHENTICATION, AND ACCESS CONTROL / IDENTITY & CREDENTIAL MANAGEMENT 246
PROTECT / IDENTITY MANAGEMENT, AUTHENTICATION, AND ACCESS CONTROL / IDENTITY BINDING TO CREDENTIALS 248
PROTECT / IDENTITY MANAGEMENT, AUTHENTICATION, AND ACCESS CONTROL / AUTHENTICATION 249
PROTECT / IDENTITY MANAGEMENT, AUTHENTICATION, AND ACCESS CONTROL / IDENTITY ASSERTIONS 252
PROTECT / IDENTITY MANAGEMENT, AUTHENTICATION, AND ACCESS CONTROL / ACCESS AUTHORIZATIONS 253
PROTECT / IDENTITY MANAGEMENT, AUTHENTICATION, AND ACCESS CONTROL / PHYSICAL ACCESS 257
PROTECT / AWARENESS AND TRAINING / USER AWARENESS & TRAINING 258
PROTECT / AWARENESS AND TRAINING / SPECIALIZED ROLE AWARENESS & TRAINING 263
PROTECT / DATA SECURITY / PROTECTION OF DATA AT REST 274
PROTECT / DATA SECURITY / PROTECTION OF DATA IN TRANSIT 278
PROTECT / DATA SECURITY / PROTECTION OF DATA IN USE 279
PROTECT / DATA SECURITY / DATA BACKUP 281
PROTECT / PLATFORM SECURITY / CONFIGURATION MANAGEMENT 282
PROTECT / PLATFORM SECURITY / SOFTWARE MAINTENANCE & REPLACEMENT 291
PROTECT / PLATFORM SECURITY / HARDWARE MAINTENANCE 294
PROTECT / PLATFORM SECURITY / LOG RECORD GENERATION 295
PROTECT / PLATFORM SECURITY / UNAUTHORIZED SOFTWARE INSTALLATION & EXECUTION 298
PROTECT / PLATFORM SECURITY / SECURE SYSTEMS DEVELOPMENT PRACTICES 301
PROTECT / PLATFORM SECURITY / TECHNOLOGY OPERATIONS, SERVICE, & SUPPORT 311
PROTECT / TECHNOLOGY INFRASTRUCTURE RESILIENCE / LOGICAL ACCESS PROTECTIONS 313
PROTECT / TECHNOLOGY INFRASTRUCTURE RESILIENCE / ENVIRONMENTAL THREAT PROTECTIONS 321
PROTECT / TECHNOLOGY INFRASTRUCTURE RESILIENCE / RESILIENCE MEASURES 322
PROTECT / TECHNOLOGY INFRASTRUCTURE RESILIENCE / CAPACITY MANAGEMENT 324
DETECT / CONTINUOUS MONITORING / NETWORK MONITORING 327
DETECT / CONTINUOUS MONITORING / PHYSICAL ENVIRONMENT MONITORING 333
DETECT / CONTINUOUS MONITORING / PERSONNEL ACTIVITY MONITORING 334
DETECT / CONTINUOUS MONITORING / SERVICE PROVIDER MONITORING 337
DETECT / CONTINUOUS MONITORING / HARDWARE, SOFTWARE, & DATA MONITORING 339
DETECT / ADVERSE EVENT ANALYSIS / POTENTIALLY ADVERSE EVENT ANALYSIS 342
DETECT / ADVERSE EVENT ANALYSIS / EVENT INFORMATION CORRELATION 344
DETECT / ADVERSE EVENT ANALYSIS / IMPACT & SCOPE DETERMINATION 347
DETECT / ADVERSE EVENT ANALYSIS / EVENT INFORMATION SHARING 349

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

DETECT / Adverse Event Analysis / Contextual Analysis 350
DETECT / Adverse Event Analysis / Incident Declaration 351
RESPOND / Incident Management / Response Plan Execution 353
RESPOND / Incident Management / Incident Triage & Validation 354
RESPOND / Incident Management / Incident Categorization & Prioritization 355
RESPOND / Incident Management / Incident Escalation 356
RESPOND / Incident Management / Recovery Initiation 357
RESPOND / Incident Analysis / Incident Analysis & Root Cause Determination 359
RESPOND / Incident Analysis / Investigation Documentation 360
RESPOND / Incident Analysis / Incident Data Collection & Preservation 362
RESPOND / Incident Analysis / Incident Magnitude Determination 364
RESPOND / Incident Response Reporting and Communication / Stakeholder Incident Notification 365
RESPOND / Incident Response Reporting and Communication / Stakeholder Incident Information Sharing 370
RESPOND / Incident Mitigation / Incident Containment 373
RESPOND / Incident Mitigation / Incident Eradication 374
RECOVER / Incident Recovery Plan Execution / Recovery Plan Execution 375
RECOVER / Incident Recovery Plan Execution / Recovery Action Performance 377
RECOVER / Incident Recovery Plan Execution / Backup & Restoration Asset Integrity 381
RECOVER / Incident Recovery Plan Execution / Post-Incident Operational Norms 382
RECOVER / Incident Recovery Plan Execution / Asset Integrity Restoration 384
RECOVER / Incident Recovery Plan Execution / End-of-Incident Determination 387
RECOVER / Incident Recovery Communication / Recovery Activity Communication 388
RECOVER / Incident Recovery Communication / Public Information Sharing 391
EXTEND / Procurement Planning and Due Diligence / Procurement Planning 392
EXTEND / Procurement Planning and Due Diligence / Prospective Third Party Due Diligence 396
EXTEND / Procurement Planning and Due Diligence / Technology & Cybersecurity Risk Assessment 401
EXTEND / Procurement Planning and Due Diligence / Product & Service Due Diligence 407
EXTEND / Third-Party Contracts and Agreements / Contract General Requirements 409
EXTEND / Third-Party Contracts and Agreements / Contract Cybersecurity-Related Requirements 412
EXTEND / Monitoring and Managing Suppliers / Ongoing Third-Party Monitoring 416
EXTEND / Monitoring and Managing Suppliers / Ongoing Third-Party Management 423
EXTEND / Relationship Termination / Termination Planning 427
EXTEND / Relationship Termination / Termination Practices 432

APPENDIX A – ABBREVIATIONS 434

APPENDIX B – KEY TERMS 435

APPENDIX C – DIAGNOSTIC STATEMENTS & IMPACT TIERS 439

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

CYBER RISK INSTITUTE

CRI Profile ver. 2.2 Guidebook Change Log

Section	Change	Page Number(s)
All	• No changes were made to the Profile Diagnostic Statements or structure (Functions, Categories, or Subcategories) from CRI Profile ver. 2.1. The CRI Profile ver. 2.2 remains fully compatible with the Profile Maturity Model ver. 2.1.	All
Impact Tiering Questionnaire	• Question 1.1.a in the Impact Tiering Questionnaire was clarified with respect to sector critical infrastructure designation.	N/A
Diagnostic Statement Reference	• The Examples of Effective Evidence for Evidence Package EEE-024, Supplier Collaboration and Security Initiatives, have been corrected for Diagnostic Statements EX.CN-02.01, EX.MM-01.03, and EX.MM-02.03.	12 - 431
Diagnostic Statement Reference	• Added the Examples of Effective Evidence Package EEE-113, Investment and Procurement Review for Architectural Consistency, for Diagnostic Statement GV.RM-08.04.	86
CRI Profile Mappings Catalog	• 13 Profile mappings were added, 3 mappings were updated, and one was removed. Refer to the CRI Profile Mapping Catalog document for details.	N/A
CRI Profile v2.2 Excel F	• The Financial Services Mapping References column in the Profile Structure view was updated to reflect the new/changed Profile mappings.	N/A

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

CYBER RISK INSTITUTE

ABOUT THE CRI PROFILE GUIDEBOOK

Background

The CRI Profile ("the Profile")[1], produced through public-private collaboration[2], is an industry-backed, consolidated approach to assessing cybersecurity, resilience, and efficacy. The Profile is an ever-evolving and concise list of assessment questions curated based on the intersection of global regulations and cyber standards, such as the International Standards Organization (ISO)[3] and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[4] More specifically, the Profile consolidates 2,500+ regulatory, official guidance and other supervisory provisions worldwide into a simple framework of 318 diagnostic statements upon which financial institutions can rely upon. The Cyber Risk Institute (CRI), a non-for-profit coalition of financial institutions and trade associations, houses and maintains the Profile and implementing guidance. The Profile provides a benchmark for cybersecurity and resiliency in the financial services industry.

Purpose

The purpose of the *Profile Guidebook* is to (1) assist organizations in implementing the Profile and (2) drive consistency when completing the Profile within the financial sector. The *Profile Guidebook* provides interpretive guidance on each of the CRI Profile's 318 Diagnostic Statements and examples of effective evidence to support the organization's response.

The *Profile Guidebook* is intended to be a living document based upon continued implementation and/or changes to the Profile.[5] CRI will update and maintain the *Profile Guidebook* as necessary to reflect these changes.

Intended Audience

The CRI Profile is designed for all financial institutions, financial services companies, financial firms, and their third-party providers. A broad cross-section of the financial services industry—banking, insurance, asset management, market utilities, broker-dealers—designed the Profile to scale across organizations of varying complexity, interconnectedness, and criticality. The Profile may be used in

---

[1] Refer to and download the Profile on the CRI website: www.cyberriskinstitute.org.

[2] The CRI Profile was originally produced through a coalition of trade associations gathered under the Financial Services Sector Coordinating Council (FSSCC). Over 150 financial institutions, ranging from community banks and credit unions to large multi-national banks, investment firms, and insurance institutions, participated in the development of the Profile. To aid in further development of the Profile, these institutions solicited and received input and direction from a myriad of U.S. and international financial services regulatory bodies, and the National Institute of Standards and Technology (NIST) hosted a workshop, to aid in further development of the Profile.

[3] ISO is an independent, non-governmental, international organization that brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant, international standards. The ISO 27000 series provides control standards specific to information security.

[4] Refer to the Framework for Improving Critical Infrastructure Cybersecurity, more commonly known as the "NIST Cybersecurity Framework" or "NIST CSF" on the NIST website.

[5] CRI is committed to updating the Profile regularly by releasing major revisions every 2 to 3 years.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

multiple ways, from self-assessment and third-party risk management, to providing a common supervisory engagement approach for financial services. Any organization engaged in completion or review of an organization's cyber risk management program can use and leverage the *Profile Guidebook* to implement the Profile, including information security risk, cybersecurity, legal, audit and prudential regulator examination staff.

Contents

This *Profile Guidebook* is intended to provide guidance for responding to all 318 Diagnostic Statements, outlined by Function, Category, and Subcategory. Users can navigate to each of the 318 Diagnostic Statements using the navigation pane and table of contents. The reference information for each Diagnostic Statement includes the following:

- **Subject Tags:** The Diagnostic Statement Subject Tags from the Profile ver. 2.0 Excel spreadsheet file have been added to the reference information. The Subject Tags can be used to search the document for Diagnostic Statements related to over 100 topic areas.
- **Response Guidance:** Interpretive guidance with additional detail on each Diagnostic Statement to help organizations understand the intent of the statement for purposes of response.
- **Examples of Effective Evidence:** The CRI Profile ver. 2.2 and the Maturity Model provide examples of evidence that may be effective in assessing and demonstrating the maturity level of a given Diagnostic Statement. To facilitate the organization and presentation of evidence, the examples of evidence are organized into 112 "Packages." A Package is simply a related grouping or logical "folder" of types of example evidence. For example, the Package "EEE-028 Investigation and Forensic Documentation" contains specific evidence examples such as "Standard operating procedures (SOPs) for conducting security investigations and handling forensic data" and "Chain of custody forms and logs that track the handling and analysis of forensic evidence." Each evidence Package is mapped to one or more Diagnostic Statement. The evidence Packages, their component examples of effective evidence, and their mappings to Profile Diagnostic Statements can be found in the CRI Profile ver. 2.2 spreadsheet file, the Maturity Model spreadsheet file, and the Diagnostic Statement-level guidance found in Section 2 of this document.

  A sample of the Packages and Examples of Effective Evidence for the Diagnostic Statement DE.AE-04.01 is provided below. The Package names are in bold font and the examples of evidence items for each Package are provided in the bulleted lists.

  > ***DE.AE-04.01:*** *The organization has a documented process to analyze and triage incidents to assess root cause, technical impact, mitigation priority, and business impact on the organization, as well as across the financial sector and other third-party stakeholders.*

  Examples of Effective Evidence:

  EEE-028: Investigation and Forensic Documentation

  - Standard operating procedures (SOPs) for conducting security investigations and handling forensic data.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Chain of custody forms and logs that track the handling and analysis of forensic evidence.
- Forensic toolkits and software licenses used for data analysis during investigations.
- Forensic investigation reports detailing the rigor of methods applied.
- Training certifications and other qualifications for personnel or third parties involved in forensic investigations.
- Reports from completed investigations, including methodologies, findings, and recommendations.

EEE-081: Incident Analysis and Triage Process Documentation

- Documentation of standardized processes for analyzing and triaging security incidents, including criteria for categprization and prioritization.
- Logs and reports from incident management systems showing the application of triage processes in real incidents.
- After-action reviews or lessons learned documents from incidents, highlighting the effectiveness of analysis and triage procedures.
- Continuous improvement plans based on feedback and performance metrics from incident analysis activities.

EEE-100: Resilience Testing and Business Impact Documentation

- Resilience testing plans and procedures, including objectives and expected outcomes.
- Business Impact Assessment (BIA) reports that evaluate the potential effects of disruptions on business operations.
- Records of resilience testing exercises, including scenarios, execution, and lessons learned.
- Documentation of updates to resilience plans based on testing outcomes and BIA findings.
- Stakeholder feedback on the organization's resilience and the impact of potential business disruptions.

Consider the following factors when selecting and assessing evidence:

- Evidence (including screenshots and embedded documents within standards or processes) should not be older than a defined period of time (e.g., 12 to 15 months).
- Implemented means fully operational, tested, and monitored – not just that a tool is installed on the hardware.
- The examples of effective evidence provided for each Diagnostic Statement are not intended to be exclusive, exhaustive, or all-inclusive, but simply examples of what could be effective in demonstrating compliance and the accuracy of the selected maturity level. Certain examples

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

provided may not be relevant to a given organization or may not provide as much evidentiary value as a different piece of evidence.

- Profile users should consider the sufficiency of the evidence provided to adequately support the asserted response relative to the resources and investment necessary to produce the evidence. There should be no expectation that all, or even most, of the examples of effective evidence provided would be necessary or warranted (or even advised) to support the organization's assessment assertions.

For a full listing of the Profile Diagnostic Statements and the Impact Tiers associated with each statement, refer to Appendix C.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GETTING STARTED

Determine Your Organization's Impact Tier

The Profile segments the financial services sector into four tiers of criticality. Each tier corresponds with the impact that an organization would have on the global, national, sector, or local market if substantially impacted by a cybersecurity event. Complete the Impact Tiering Questionnaire, consisting of 9 questions, to determine an organization's "Impact Tier":

Tier 1: National/Super-National Impact – These institutions are designated *most critical* by one or more global regulatory agencies and/or bodies (e.g., the Basel Committee's Global Systemically Important Bank (GSIB) designation or Executive Order 13636's Section 9 designation). This category assumes the gross cyber risk exposure of an institution or service categorized as Tier 1 would have the most potential adverse impact to the overall stability of a national economy, and potentially, the global market.

Tier 2: Subnational Impact – These institutions provide mission critical services with millions of customer accounts. This category assumes the gross cyber risk exposure of an institution or service would have the potential for a substantial adverse impact to the financial services sector and subnational regional economy but does not rise to the level of Tier 1.

Tier 3: Sector Impact – These institutions have a high degree of interconnectedness, with certain institutions acting as key nodes within, and for, the sector. The nature of the services that these institutions provide to the sector plays a significant role in determining their criticality.

Tier 4: Localized Impact – These institutions have a limited impact on the overall financial services sector and national economy. Typical characteristics include: (a) institutions with a local presence and less than 1 million customers (e.g., community banks, state banks) and (b) providers of low criticality services.

Assess Your Organization's Cyber Risk Management Program Using the Profile's Diagnostic Statements

The Profile includes seven overarching Functions for assessing an organization's cyber risk management program: 1) Governance, 2) Identify, 3) Detect, 4) Protect, 5) Respond, 6) Recover, and 7) Supply Chain/Dependency Management. Each Function is subdivided into specific concept Categories and Subcategories, which are designed to reflect an element of an effective cyber risk management program. Each Subcategory is associated with at least one Diagnostic Statement to assess the organization's cyber risk management program. After completing the Impact Tiering Questionnaire, organizations respond to a certain number of Diagnostic Statements corresponding to their Impact Tier.

Tier 1: National/Super-National Impact includes 318 Diagnostic Statements

Tier 2: Subnational Impact includes 311 Diagnostic Statements

Tier 3: Sector Impact includes 282 Diagnostic Statements

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Tier 4: Localized Impact includes 208 Diagnostic Statements

Response Key

Organizations note the outcome of their assessment by selecting between eight potential Diagnostic Statement responses, with the default response is set to "To Be Assessed." The potential Diagnostic Statement responses include:

1) **Yes:** All of the control outcome(s) described in the Profile Diagnostic Statement are assessed and/or tested on a regular basis and are demonstrated to have been designed and operating reliably in the organizational environment.
2) **No:** The control outcome(s) described in the Profile Diagnostic Statement have not been meaningfully improved.
3) **Partial:** A meaningful subset of the control outcome(s) described in the Profile Diagnostic Statement are assessed and/or tested on a regular basis and are demonstrated to have been designed and operating reliably in the organizational environment.
4) **Not Applicable:** The Profile Diagnostic Statement has been determined to be not applicable to the assessment and will not be counted towards any intermediate or total result.
5) **Yes-Risk Based:** The control outcome(s) described in the Profile Diagnostic Statement are assessed and/or tested on a regular basis and are demonstrated to have been designed and operating reliably for the highest-risk assets, or highest-risk control functions, in organizational environment.
6) **Yes-Compensating Control:** An institution might select this response if it meets the intent of the Diagnostic Statement by using compensating controls.
7) **Not Tested:** An institution might select this response if it has yet to test controls associated with the Diagnostic Statement.
8) **I don't know:** An individual assessment user might select this response as a placeholder/note to check with other relevant stakeholders within the institution to determine the most accurate response.

Tips for Completing the Profile and for Use with the Examination Staff

Organizations can use the *Profile Guidebook* to determine the appropriate Diagnostic Statement response as detailed above. Organizations should collect and maintain documentation and other evidence to support their assessment and response to each Diagnostic Statement. The following tips may be considered in using the *Profile Guidebook*:

- Socialize the use and benefits of the Profile within your organization with management, internal audit, third-party oversight, legal, and other business lines, as well as with your regulators.
- Implement an independent review of completed Profile responses and evidence prior to regulatory submission.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Evidence (including screen shots and embedded documents within standards or processes) must not be older than 12 to 15 months.
- Implemented means fully operational, tested, and monitored—not just that the tool is loaded on the hardware.
- Document all areas of challenge and response to challenge (date, who challenged, who responded, and if challenge caused change to response).
- Implement an ongoing monitoring process to address Profile changes based on trigger events as defined in the organization's risk management framework and provide updates to internal audit and regulators as they occur.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

CYBER RISK INSTITUTE

DIAGNOSTIC STATEMENT REFERENCE

GOVERN / Organizational Context / Organizational Mission

GV.OC-01.01: Technology and cybersecurity strategies, architectures, and programs are formally governed to align with and support the organization's mission, objectives, priorities, tactical initiatives, and risk profile.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #architecture | #mission_and_strategy | #risk_management

Response Guidance:

Describe how the organization's mission, objectives, and activities establish priorities for the technology and cybersecurity strategies, architectures, and programs and communicates those priorities. Response should include documentation, such as the organizational mission statement, cybersecurity and technology program, strategies, architectures, aligned target operating model (i.e., desired state of operations considering the organization's role in critical infrastructure) and related documents supporting the establishment and communication of priorities for the organizational mission, objectives, and activities.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.
- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-002: Board Governance and IT Oversight Documentation

- Board of Directors' charter and governance guidelines.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Copies of presentations, reports, and minutes from board meetings and committees related to IT and cybersecurity.
- Records of decisions and actions taken regarding IT governance.
- Policy documents on roles and responsibilities of governance bodies.
- Compliance reports related to governance policies and practices.

EEE-003: Strategic Objectives and Planning Documents

- Documentation ot the organization's mission statement.
- Strategic plan outlining the organization's objectives and key results.
- Executive summaries of strategic goals related to IT and cybersecurity.
- Performance reports against strategic objectives.
- Communications from leadership on strategic direction and priorities.

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-005: Risk Appetite Tolerance, and Strategy Alignment Documents

- Risk appetite statements approved by the board or executive management.
- Risk tolerance levels defined for different categories of risk.
- Documentation on how risk appetite influences decision-making and strategy.
- Reports on risk exposures compared to the defined risk appetite.
- Updates or revisions to risk appetite and tolerance based on changing conditions.

GOVERN / Organizational Context / Stakeholder Risk Management Expectations

GV.OC-02.01: The organization's obligation to its customers, employees, and stakeholders to maintain safety and soundness, while balancing size and complexity, is reflected in the organization's risk management strategy and framework, its risk appetite and risk tolerance statements, and in a risk-aware culture.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #mission_and_strategy | #risk_appetite_/_tolerance | #risk_management

Response Guidance:

The organization's risk management processes should align the organization's risk appetite with business objectives. The organization should consider their obligations to protect its customer, employee, and stakeholder information from being exposed to excessive risks that may reduce confidence in the organization or sector. Organization management should define and document their

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

risk tolerance and risk appetite statements, and promote a risk-aware culture in order to maintain risk exposure within the established risk tolerance limits.

Responses should provide information on the organization's risk tolerance and risk appetite statements including supporting details on how the organization considers their obligations to customers, employees, and stakeholders. Describe the organizations risk-aware culture and how they assess, monitor, report, and manage identified risks.

Examples of Effective Evidence:

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-005: Risk Appetite Tolerance, and Strategy Alignment Documents

- Risk appetite statements approved by the board or executive management.
- Risk tolerance levels defined for different categories of risk.
- Documentation on how risk appetite influences decision-making and strategy.
- Reports on risk exposures compared to the defined risk appetite.
- Updates or revisions to risk appetite and tolerance based on changing conditions.

EEE-006: Cybersecurity, Culture, and Training Record Documents

- Employee cybersecurity awareness survey results.
- Training attendance logs for cybersecurity and IT policy courses.
- Assessments of organizational culture regarding security practices.
- Feedback and improvement reports following culture assessments.
- Records of cultural change initiatives related to cybersecurity.

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

EEE-104: Risk Tolerance and Management Practice Integration Documentation

- Documentation of the organization's risk tolerance levels and how these are integrated into risk management practices.
- Records of risk assessments that consider the organization's risk tolerance when determining mitigation strategies.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Reports to management and the board on risk exposures in relation to the defined risk tolerance.
- Reviews of risk management practices to ensure they remain aligned with the organization's risk tolerance.

GV.OC-02.02: Technology and cybersecurity risk management strategies identify and communicate the organization's role within the financial services sector as a component of critical infrastructure.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Subject Tags: #business_impact_analysis | #critical_infrastructure | #mission_and_strategy | #risk_management | #roles_and_responsibilities

Response Guidance:

The United States Department of Homeland Security has identified the financial services sector as a critical infrastructure sector. Similarly, the sector has been identified as critical infrastructure by the European Programme for Critical Infrastructure Protection and the UK's Centre for Protection of National Infrastructure (CPNI) . Further, the U.S. Government has identified and prioritized certain large organizations where a cybersecurity incident could result in catastrophic regional or national effects on economic or national security. Cybersecurity strategies should recognize the organization's role in the financial sector as well as dependencies on other critical infrastructures .

Responses should include how the technology and cybersecurity risk management strategies have both identified and communicated the organization's role within the sector as a component of critical infrastructure within the financial services Industry. For example, an organization may be a main provider of wholesale payments, clearing and settlement or some other critical function that could be detrimental to the industry and the economy if the organization is not able to function. Include whether the organization is a member of the Analysis and Resilience Center for Systemic Risk (ARC), the Bank of England Cross Market Operational Resilience Group (CMORG) or similar organization to address critical sector impacts.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-002: Board Governance and IT Oversight Documentation

- Board of Directors' charter and governance guidelines.
- Copies of presentations, reports, and minutes from board meetings and committees related to IT and cybersecurity.
- Records of decisions and actions taken regarding IT governance.
- Policy documents on roles and responsibilities of governance bodies.
- Compliance reports related to governance policies and practices.

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-005: Risk Appetite Tolerance, and Strategy Alignment Documents

- Risk appetite statements approved by the board or executive management.
- Risk tolerance levels defined for different categories of risk.
- Documentation on how risk appetite influences decision-making and strategy.
- Reports on risk exposures compared to the defined risk appetite.
- Updates or revisions to risk appetite and tolerance based on changing conditions.

EEE-007: Legal, Regulatory, and Compliance Management Documentation

- Compliance audit reports for relevant laws and regulations (e.g., GDPR, HIPAA).
- Documentation of legal advice received on cybersecurity matters, to include determinations of incident materiality.
- Records of regulatory filings and notices related to IT and cybersecurity.
- Updates to policies and procedures in response to legal and regulatory changes.
- Training records on legal and regulatory requirements for IT staff.

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

EEE-015: Sector-Wide Dependency and Impact Analysis Documentation

- Analysis reports detailing the dependencies within the organization's sector and potential vulnerabilities.
- Tools or software used to evaluate the criticality of external partners and suppliers.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Summaries from workshops and exercises aimed at understanding the sector-wide impact of external disruptions.
- Reports on how regulatory changes could affect critical external dependencies.
- Real-time dashboards for monitoring geopolitical events that may impact the sector.

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-104: Risk Tolerance and Management Practice Integration Documentation

- Documentation of the organization's risk tolerance levels and how these are integrated into risk management practices.
- Records of risk assessments that consider the organization's risk tolerance when determining mitigation strategies.
- Reports to management and the board on risk exposures in relation to the defined risk tolerance.
- Reviews of risk management practices to ensure they remain aligned with the organization's risk tolerance.

GV.OC-02.03: Technology and cybersecurity risk management strategies identify and communicate the organization's role as it relates to other critical infrastructure sectors outside of the financial services sector and the interdependency risks.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Subject Tags: #business_impact_analysis | #critical_infrastructure | #mission_and_strategy | #risk_management

Response Guidance:

The Board or Committee should be familiar with how relevant government agencies determine critical infrastructure. For example, in the United States, the Department of Homeland Security's critical infrastructure list and critical functions set are used to identify relevant sectors. In the United Kingdom the Centre for the Protection of National Infrastructure defines critical national infrastructure.

Responses should include the Board or Committee's awareness of any critical infrastructure that the organization's services or activities could impact due to a cyber breach or service degradation. Large organizations play a particularly important role in terms of critical infrastructure planning because of their potential systemic impact, including the potential national or global effects an adverse event could have in the financial sector and the national/global economy. Technology and cybersecurity risk

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

management strategies should recognize the organization's role with respect to critical infrastructure functions, including details on how the risk management strategies are related to other critical infrastructures outside of the financial sector (e.g., energy, communications, information technology, etc.).

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.
- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-015: Sector-Wide Dependency and Impact Analysis Documentation

- Analysis reports detailing the dependencies within the organization's sector and potential vulnerabilities.
- Tools or software used to evaluate the criticality of external partners and suppliers.
- Summaries from workshops and exercises aimed at understanding the sector-wide impact of external disruptions.
- Reports on how regulatory changes could affect critical external dependencies.
- Real-time dashboards for monitoring geopolitical events that may impact the sector.

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

GOVERN / Organizational Context / Legal, Regulatory, & Contractual Requirements

GV.OC-03.01: The organization's technology and cybersecurity strategy, framework, and policies align and are consistent with the organization's legal, statutory, contractual, and regulatory obligations and ensure that compliance responsibilities are unambiguously assigned.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #compliance | #mission_and_strategy | #policy_management

Response Guidance:

The Gramm-Leach-Bliley Act and its implementing regulations, including the Guidelines Establishing Standards for Safeguarding Customer Information is the seminal set of legal expectations as it relates to information security for financial institutions in the United States. Other jurisdictions will have additional legal and regulatory obligations in place. Regulatory guidance and/or legal requirements may apply based on products, services, and legal structure. Furthermore, organizations will have contractual obligations with vendors, government agencies, and other third-party service providers that should be tracked for compliance with established responsibilities.

Provide information on how new or enhanced technology and cybersecurity regulations and contractual obligations are published (trigger event), and how technology and cybersecurity strategies, frameworks, and policies are reviewed and updated to ensure regulatory and contractual obligation alignment. Responses should describe any existing efforts within the organization that may map regulatory and contractual requirements to existing policies, procedures, and controls. Provide information regarding any the organizations processes for identifying, tracking, and overseeing regulatory and contractual requirements. Roles and responsibilities should be clearly defined and unambiguously assigned for technology and cybersecurity. Provide information on how the organization ensures responsibilities are unambiguously assigned (e.g., compliance responsibility assignment matrix, RACI charts).

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.
- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-002: Board Governance and IT Oversight Documentation

- Board of Directors' charter and governance guidelines.
- Copies of presentations, reports, and minutes from board meetings and committees related to IT and cybersecurity.
- Records of decisions and actions taken regarding IT governance.
- Policy documents on roles and responsibilities of governance bodies.
- Compliance reports related to governance policies and practices.

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-007: Legal, Regulatory, and Compliance Management Documentation

- Compliance audit reports for relevant laws and regulations (e.g., GDPR, HIPAA).
- Documentation of legal advice received on cybersecurity matters, to include determinations of incident materiality.
- Records of regulatory filings and notices related to IT and cybersecurity.
- Updates to policies and procedures in response to legal and regulatory changes.
- Training records on legal and regulatory requirements for IT staff.

EEE-008: Customer Data Privacy and Data Protection Documentation

- Published privacy policy detailing how customer data is handled and protected.
- Consent forms and records of customer approvals for data processing.
- Data Protection Impact Assessments (DPIAs) for new projects involving personal data.
- Records of privacy policy reviews and updates.
- Documentation of customer notifications in the event of a data breach.

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

GV.OC-03.02: The organization implements and maintains a documented policy or policies that address customer data privacy that is approved by a designated officer or the organization's appropriate governing body (e.g., the Board or one of its committees).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #compliance | #policy_management

Response Guidance:

Describe how the various policies and standards in place are designed to protect customer privacy and comply with local laws. Indicate how these documents describe security and safeguarding of information generated and obtained in the course of executing business activities. Identify who in the organization is responsible for maintaining privacy-related programs, documents, and compliance activities.

Examples of Effective Evidence:

EEE-007: Legal, Regulatory, and Compliance Management Documentation

- Compliance audit reports for relevant laws and regulations (e.g., GDPR, HIPAA).
- Documentation of legal advice received on cybersecurity matters, to include determinations of incident materiality.
- Records of regulatory filings and notices related to IT and cybersecurity.
- Updates to policies and procedures in response to legal and regulatory changes.
- Training records on legal and regulatory requirements for IT staff.

EEE-008: Customer Data Privacy and Data Protection Documentation

- Published privacy policy detailing how customer data is handled and protected.
- Consent forms and records of customer approvals for data processing.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Data Protection Impact Assessments (DPIAs) for new projects involving personal data.
- Records of privacy policy reviews and updates.
- Documentation of customer notifications in the event of a data breach.

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.
- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

EEE-098: Customer Data Privacy and Compliance Documents

- Privacy policies and procedures that detail how customer data is protected and used in compliance with relevant laws and regulations.
- Records of privacy compliance audits, including findings and corrective actions taken.
- Documentation of customer consent and data handling practices, demonstrating adherence to privacy principles.
- Training records for staff on data privacy regulations and customer data handling procedures.
- Incident logs related to customer data privacy, including any breaches and the organization's response.

GOVERN / Organizational Context / Stakeholder Service Expectations

GV.OC-04.01: The organization maintains an inventory of key internal assets, business functions, and external dependencies that includes mappings to other assets, business functions, and information flows.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #architecture | #asset_management | #data_flow | #dependency_management | #network_diagrams | #resilience

Response Guidance:

Describe the processes and tools related to the maintenance of an inventory of internal and externally managed assets and business functions. The identification of dependencies has become increasingly important in today's networked environments because applications and services rely on a variety of supporting services. Dependencies and interdependencies among applications and services should be noted to support activities such as conducting code reviews, security assessments, modifications to firewall/network policies, and testing. Include in the response the mapping of internal assets and business functions to other assets, business functions, and information flows.

Consider the organization's operational resilience as it relates to the inventory of critical assets and business services within the organization's inventory. The list should identify systemically important

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

business services and associated mappings to assets and dependencies to satisfy operational resilience requirements and help manage disruptions to the safety and soundness of the market.

Examples of Effective Evidence:

EEE-010: IT Asset Management and Business Function Mapping Documentation

- Inventory list of IT assets, including hardware, software, and data.
- Business function catalog that maps key assets to their corresponding business process.
- Asset ownership and stewardship records indicating who is responsible for specific assets.
- Lifecycle management records for assets, showing purchase dates, warranty periods, and disposal information.
- Integration diagrams showing how assets interact within the business's technology ecosystem.

EEE-011: External Dependencies and Risk Assessment Documents

- Diagrams of network architecture showing connections to external systems and services.
- Contracts and service level agreements (SLAs) with key vendors and service providers.
- Risk assessments of external dependencies highlighting potential impact on business operations.
- Documentation of alternative vendors and backup resources in case of primary vendor failure.
- Incident reports related to external dependencies, including response and resolution details.

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.
- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

GV.OC-04.02: The organization documents the business processes that are critical for the delivery of services and the functioning of the organization, and the impacts to the business if those processes are degraded or not functioning.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #business_impact_analysis | #business_process | #critical_infrastructure | #dependency_management | #resilience | #security_logging_monitoring_and_alerting | #technology_availability

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

As part of managing risks, the organization should understand existing business processes and identify which processes are critical for the delivery of services and functioning of the organization. Describe the organization's approach to identify critical business processes. The response should include impacted upstream and downstream systems and services and the potential impacts on internal and external stakeholders.

Examples of Effective Evidence:

EEE-012: Critical Business Process and Recovery Documentation

- Process and informatioin flow diagrams for critical business operations.
- Business impact analyses that identify and prioritize critical processes.
- Procedures and guidelines for maintaining and operating critical processes.
- Performance metrics and monitoring reports for critical processes.
- Recovery plans for critical business processes in the event of disruption.

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.
- Business continuity plan outlining procedures for maintaining service delivery during disruptions.
- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.
- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.
- Contingency plans detailing alternative service delivery methods.
- Training records for staff on resilience and continuity procedures and their roles during incidents.

EEE-016: Recovery Objectives and Strategic Alignment Documentation

- Tools and templates used for formulating recovery strategies that support business objectives.
- A matrix aligning recovery time and point objectives with business priorities.
- Documentation from strategic planning sessions focused on recovery objectives.
- Signed approvals from management endorsing the proposed recovery strategies.
- Periodic review reports assessing the alignment of recovery objectives with business needs.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GV.OC-04.03: Resilience requirements to support the delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, and normal operations).

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Subject Tags: #business_impact_analysis | #business_process | #critical_infrastructure | #data_backup | #resilience | #review_assessment_and_testing

Response Guidance:

Describe the establishment of technology cyber resilience requirements to support delivery of critical services for all operating states (e.g., under duress/attack, during recovery, normal operations). Include documentation or catalog of critical services inventory and related dependencies. Describe reasonably expected scenarios/conditions of alternative operating states (e.g., ransomware attack, extended site recovery, site loss, etc.)

Examples of Effective Evidence:

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.
- Business continuity plan outlining procedures for maintaining service delivery during disruptions.
- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.
- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.
- Contingency plans detailing alternative service delivery methods.
- Training records for staff on resilience and continuity procedures and their roles during incidents.

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.
- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-016: Recovery Objectives and Strategic Alignment Documentation

- Tools and templates used for formulating recovery strategies that support business objectives.
- A matrix aligning recovery time and point objectives with business priorities.
- Documentation from strategic planning sessions focused on recovery objectives.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Signed approvals from management endorsing the proposed recovery strategies.
- Periodic review reports assessing the alignment of recovery objectives with business needs.

EEE-029: Critical Function Resilience Documentation

- Plans that specifically address the continuity and resilience of critical business functions.
- Dashboards or reports that monitor the health and resilience of critical functions.
- Definitions of measures used to manage and assess resilience (RPO, RTO, MTO, Impact Tolerance, etc.)
- Documentation of resilience requirements integrated into the design of new services or processes.
- Evaluations or audits of the resilience program, highlighting strengths and areas for improvement.

EEE-058: Resilience Mechanism Validation and Feedback Documentation

- Plans and procedures for implementing resilience mechanisms across IT systems and business processes.
- Business- and associated system-level requirements for resilience.
- Architecture and design documentation detailing resilience deisgn factors and considerations.
- Schedules and reports from testing and exercises designed to validate the effectiveness of resilience mechanisms.
- Change management documentation related to the enhancement of resilience mechanisms.
- Lessons learned and improvement plans derived from resilience testing activities.
- Stakeholder feedback on the organization's resilience capabilities, gathered through surveys or interviews.

EEE-078: Resilience Testing and Infrastructure Redundancy Documentation

- Documentation of resilience testing plans and procedures, including objectives, scenarios, and expected outcomes.
- Test reports summarizing the results of resilience testing exercises, highlighting strengths and areas for improvement.
- Infrastructure redundancy designs and implementation records, showing failover capabilities and backup systems.
- Change management records documenting updates or enhancements made to improve infrastructure redundancy.
- Stakeholder feedback on the organization's resilience and redundancy capabilities, gathered after testing or actual events.

EEE-106: Recovery Objectives Critical Infrastructure Documentation

- Documentation of recovery objectives for critical infrastructure and how these align with business continuity goals.
- Critical infrastructure analysis reports that assess the resilience and recovery capabilities of essential systems.
- Records of alignment discussions or decisions between recovery objectives and business needs.
- Audit reports evaluating the alignment of recovery objectives with the criticality of infrastructure components.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-107: Data Recovery and Information Flow Mapping Documentation

- Data recovery strategy documents that outline procedures for restoring lost or corrupted data.
- Information flow maps that illustrate how data moves through the organization, informing recovery planning.
- Test reports from data recovery exercises, demonstrating the ability to restore data in line with recovery strategies.
- Documentation of changes to data recovery strategies based on new business processes or technologies.
- Training records for IT staff on data recovery procedures and information flow considerations.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

GV.OC-04.04: The organization prioritizes the resilience design, planning, testing, and monitoring of systems and other key internal and external dependencies according to their criticality to the supported business functions, enterprise mission, and to the financial services sector.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #asset_management | #business_impact_analysis | #business_process | #critical_infrastructure | #dependency_management | #resilience | #security_logging_monitoring_and_alerting | #technology_availability

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

The organization should prioritize assets according to their criticality and classification, which will guide decisions regarding internal controls and processes to effectively manage resiliency. The organization should understand the interdependencies between systems and business processes to prioritize system resiliency monitoring and processes.

Responses should describe how the organization has prioritized the resilience planning, design, testing, and monitoring of systems according to their criticality to the supported business functions, enterprise mission, and to the financial services sector. Highlight tools used and how risk is assessed.

Examples of Effective Evidence:

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.
- Business continuity plan outlining procedures for maintaining service delivery during disruptions.
- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.
- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.
- Contingency plans detailing alternative service delivery methods.
- Training records for staff on resilience and continuity procedures and their roles during incidents.

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.
- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-016: Recovery Objectives and Strategic Alignment Documentation

- Tools and templates used for formulating recovery strategies that support business objectives.
- A matrix aligning recovery time and point objectives with business priorities.
- Documentation from strategic planning sessions focused on recovery objectives.
- Signed approvals from management endorsing the proposed recovery strategies.
- Periodic review reports assessing the alignment of recovery objectives with business needs.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

EEE-029: Critical Function Resilience Documentation

- Plans that specifically address the continuity and resilience of critical business functions.
- Dashboards or reports that monitor the health and resilience of critical functions.
- Definitions of measures used to manage and assess resilience (RPO, RTO, MTO, Impact Tolerance, etc.)
- Documentation of resilience requirements integrated into the design of new services or processes.
- Evaluations or audits of the resilience program, highlighting strengths and areas for improvement.

EEE-058: Resilience Mechanism Validation and Feedback Documentation

- Plans and procedures for implementing resilience mechanisms across IT systems and business processes.
- Business- and associated system-level requirements for resilience.
- Architecture and design documentation detailing resilience deisgn factors and considerations.
- Schedules and reports from testing and exercises designed to validate the effectiveness of resilience mechanisms.
- Change management documentation related to the enhancement of resilience mechanisms.
- Lessons learned and improvement plans derived from resilience testing activities.
- Stakeholder feedback on the organization's resilience capabilities, gathered through surveys or interviews.

EEE-061: Service Recovery and Critical Operations Resumption Documentation

- Procedures and checklists for resuming services and recovering critical operations after an incident.
- Prioritization lists that identify critical services and operations for recovery efforts.
- Test results and reports from service resumption drills and recovery exercises.
- Service level agreements (SLAs) with vendors that include provisions for rapid service resumption.
- Documentation of alternative processes and workarounds to be used when primary operations are disrupted.

EEE-079: Capacity Planning and Resource Utilization Documentation

- Capacity planning strategies and models that forecast infrastructure and resource needs based on business growth and demand.
- Utilization monitoring reports and dashboards that track the usage of IT resources and infrastructure.
- Documentation of actions taken to address capacity constraints or optimize resource utilization.
- Reviews or assessments of capacity planning and utilization monitoring practices, identifying opportunities for optimization.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

GOVERN / Organizational Context / Organizational Service Dependencies

GV.OC-05.01: The organization identifies, assesses, and documents the key dependencies, interdependencies, and potential points of failure to support the delivery of critical services (e.g., systems, business processes, workforce, third parties, facilities, etc.)

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #asset_management | #business_impact_analysis | #business_process | #critical_infrastructure | #dependency_management | #staffing_and_resource_management | #third_party_risk_management | #supply_chain_management

Response Guidance:

In order to plan and assess for enterprise resilience, the organizations should identify, assess, and document internal and external dependencies to understand upstream and downstream affects of potential points of failure to critical services (systems, business processes, third parties, facilities, etc.).

Responses should describe the organizations processes to identify, assess, and document internal and external dependencies. Dependency evaluation and management processes should consider internal and external dependencies for critical services (information systems, data processing facilities, third party providers, business processes, etc.). Include considerations of backup systems and facilities, and third party service providers on retainer contracts.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-010: IT Asset Management and Business Function Mapping Documentation

- Inventory list of IT assets, including hardware, software, and data.
- Business function catalog that maps key assets to their corresponding business process.
- Asset ownership and stewardship records indicating who is responsible for specific assets.
- Lifecycle management records for assets, showing purchase dates, warranty periods, and disposal information.
- Integration diagrams showing how assets interact within the business's technology ecosystem.

EEE-011: External Dependencies and Risk Assessment Documents

- Diagrams of network architecture showing connections to external systems and services.
- Contracts and service level agreements (SLAs) with key vendors and service providers.
- Risk assessments of external dependencies highlighting potential impact on business operations.
- Documentation of alternative vendors and backup resources in case of primary vendor failure.
- Incident reports related to external dependencies, including response and resolution details.

EEE-012: Critical Business Process and Recovery Documentation

- Process and informatioin flow diagrams for critical business operations.
- Business impact analyses that identify and prioritize critical processes.
- Procedures and guidelines for maintaining and operating critical processes.
- Performance metrics and monitoring reports for critical processes.
- Recovery plans for critical business processes in the event of disruption.

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.
- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-015: Sector-Wide Dependency and Impact Analysis Documentation

- Analysis reports detailing the dependencies within the organization's sector and potential vulnerabilities.
- Tools or software used to evaluate the criticality of external partners and suppliers.
- Summaries from workshops and exercises aimed at understanding the sector-wide impact of external disruptions.
- Reports on how regulatory changes could affect critical external dependencies.
- Real-time dashboards for monitoring geopolitical events that may impact the sector.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-020: Vendor Contingency and Transition Planning Documents

- Contingency plans for transitioning services in case of vendor failure, including timelines and responsibilities.
- Checklists for evaluating vendor contingency and recovery capabilities during the selection process.
- Documentation of transition exercises or drills conducted to test the effectiveness of contingency plans.
- Vendor exit strategy documents that outline procedures for terminating relationships while maintaining operational continuity.
- Records of vendor performance issues that triggered contingency or transition plans.

EEE-025: Vendor Contingency and Risk Mitigation Documentation

- Contingency plans that outline alternative solutions in case of vendor failure or service disruption.
- Risk assessments that identify potential points of failure with vendors and corresponding contingency options.
- Documentation of the evaluation and selection process for alternative vendors or solutions.
- Communication plans for engaging with alternative vendors during a contingency event.
- Test results from contingency plan exercises, demonstrating the viability of alternative solutions.

EEE-029: Critical Function Resilience Documentation

- Plans that specifically address the continuity and resilience of critical business functions.
- Dashboards or reports that monitor the health and resilience of critical functions.
- Definitions of measures used to manage and assess resilience (RPO, RTO, MTO, Impact Tolerance, etc.)
- Documentation of resilience requirements integrated into the design of new services or processes.
- Evaluations or audits of the resilience program, highlighting strengths and areas for improvement.

EEE-034: Asset Management and Inventory Oversight Documentation

- Asset management policies that outline the processes and data requirements for tracking, maintaining, and securing organizational assets.
- Inventory lists or databases of assets, including hardware, software, data, and intellectual property, with assigned custodians or owners.
- Change logs or records of asset transfers, disposals, and acquisitions.
- Technical documentation and configuration of automated inventory discovery and management tools.
- Reports from periodic asset audits or reviews, confirming the accuracy of the inventory and compliance with the policy.
- Documentation of asset classification and labeling, indicating the criticality and sensitivity of assets.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GV.OC-05.02: The organization has prioritized its external dependencies according to their criticality to the supported enterprise mission, business functions, and to the financial services sector.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #asset_management | #business_impact_analysis | #dependency_management | #third_party_risk_management | #supply_chain_management

Response Guidance:

Describe how the organization has prioritized external dependencies according to their criticality to the supported business functions, enterprise mission, and to the financial services sector.

External dependencies (i.e., third-party dependencies) may be interconnected with, or support sector-critical systems and operations, and disruptions to the external dependency could pose a risk to both the organization and the entire financial services sector. For example, if an external dependency prevents an organization from making a significant number of payments, it could have adverse effects on financial stability. Additionally, if a payments or settlement service experienced an outage with an external dependency, it could have a significant impact on other financial services organizations.

Examples of Effective Evidence:

EEE-010: IT Asset Management and Business Function Mapping Documentation

- Inventory list of IT assets, including hardware, software, and data.
- Business function catalog that maps key assets to their corresponding business process.
- Asset ownership and stewardship records indicating who is responsible for specific assets.
- Lifecycle management records for assets, showing purchase dates, warranty periods, and disposal information.
- Integration diagrams showing how assets interact within the business's technology ecosystem.

EEE-011: External Dependencies and Risk Assessment Documents

- Diagrams of network architecture showing connections to external systems and services.
- Contracts and service level agreements (SLAs) with key vendors and service providers.
- Risk assessments of external dependencies highlighting potential impact on business operations.
- Documentation of alternative vendors and backup resources in case of primary vendor failure.
- Incident reports related to external dependencies, including response and resolution details.

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-015: Sector-Wide Dependency and Impact Analysis Documentation

- Analysis reports detailing the dependencies within the organization's sector and potential vulnerabilities.
- Tools or software used to evaluate the criticality of external partners and suppliers.
- Summaries from workshops and exercises aimed at understanding the sector-wide impact of external disruptions.
- Reports on how regulatory changes could affect critical external dependencies.
- Real-time dashboards for monitoring geopolitical events that may impact the sector.

EEE-020: Vendor Contingency and Transition Planning Documents

- Contingency plans for transitioning services in case of vendor failure, including timelines and responsibilities.
- Checklists for evaluating vendor contingency and recovery capabilities during the selection process.
- Documentation of transition exercises or drills conducted to test the effectiveness of contingency plans.
- Vendor exit strategy documents that outline procedures for terminating relationships while maintaining operational continuity.
- Records of vendor performance issues that triggered contingency or transition plans.

GV.OC-05.03: The organization defines objectives (e.g., Recovery Time Objective, Maximum Tolerable Downtime, Impact Tolerance) for the resumption of critical operations in alignment with business imperatives, stakeholder obligations, and critical infrastructure dependencies.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #architecture | #asset_management | #business_impact_analysis | #critical_infrastructure | #data_backup | #data_flow | #data_integrity | #disaster_recovery | #network_diagrams | #resilience | #roles_and_responsibilities | #security_logging_monitoring_and_alerting | #technology_availability

Response Guidance:

Describe how the organization defines objectives for resumption of critical operations (recovery time objectives, recovery point objectives). Organizations should establish an Impact Tolerance objective for critical business services that defines the maximum tolerable level and duration for a disruption. Describe how the Recovery Time Objective, Maximum Tolerable Downtime, and Impact Tolerance are designed to improve the organization’s operational resilience. Include information on the organization’s business impact analysis, the scope of critical business processes, and prioritization for recovery, among other details. Provide information on the framework and tools utilized to define objectives. Provide information on frequency of assessment and any risk-based criteria.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.
- Business continuity plan outlining procedures for maintaining service delivery during disruptions.
- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.
- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.
- Contingency plans detailing alternative service delivery methods.
- Training records for staff on resilience and continuity procedures and their roles during incidents.

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.
- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-016: Recovery Objectives and Strategic Alignment Documentation

- Tools and templates used for formulating recovery strategies that support business objectives.
- A matrix aligning recovery time and point objectives with business priorities.
- Documentation from strategic planning sessions focused on recovery objectives.
- Signed approvals from management endorsing the proposed recovery strategies.
- Periodic review reports assessing the alignment of recovery objectives with business needs.

EEE-029: Critical Function Resilience Documentation

- Plans that specifically address the continuity and resilience of critical business functions.
- Dashboards or reports that monitor the health and resilience of critical functions.
- Definitions of measures used to manage and assess resilience (RPO, RTO, MTO, Impact Tolerance, etc.)
- Documentation of resilience requirements integrated into the design of new services or processes.
- Evaluations or audits of the resilience program, highlighting strengths and areas for improvement.

EEE-106: Recovery Objectives Critical Infrastructure Documentation

- Documentation of recovery objectives for critical infrastructure and how these align with business continuity goals.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Critical infrastructure analysis reports that assess the resilience and recovery capabilities of essential systems.
- Records of alignment discussions or decisions between recovery objectives and business needs.
- Audit reports evaluating the alignment of recovery objectives with the criticality of infrastructure components.

EEE-107: Data Recovery and Information Flow Mapping Documentation

- Data recovery strategy documents that outline procedures for restoring lost or corrupted data.
- Information flow maps that illustrate how data moves through the organization, informing recovery planning.
- Test reports from data recovery exercises, demonstrating the ability to restore data in line with recovery strategies.
- Documentation of changes to data recovery strategies based on new business processes or technologies.
- Training records for IT staff on data recovery procedures and information flow considerations.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GV.OC-05.04: Recovery point objectives to support data integrity are consistent with the organization's recovery time objectives, information flow dependencies between systems, and business obligations.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #architecture | #data_backup | #data_flow | #data_integrity | #dependency_management | #disaster_recovery | #network_diagrams | #resilience

Response Guidance:

Describe how the organization's recovery point objectives support data integrity efforts are consistent with the organization's requirements for recovery of critical operations. Provide information on the impact of a cyber-attack relative to recovery point objectives.

Examples of Effective Evidence:

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.
- Business continuity plan outlining procedures for maintaining service delivery during disruptions.
- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.
- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.
- Contingency plans detailing alternative service delivery methods.
- Training records for staff on resilience and continuity procedures and their roles during incidents.

EEE-016: Recovery Objectives and Strategic Alignment Documentation

- Tools and templates used for formulating recovery strategies that support business objectives.
- A matrix aligning recovery time and point objectives with business priorities.
- Documentation from strategic planning sessions focused on recovery objectives.
- Signed approvals from management endorsing the proposed recovery strategies.
- Periodic review reports assessing the alignment of recovery objectives with business needs.

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-086: Recovery Strategy and Resilience Plan Documentation

- Documentation of the organization's recovery strategies, including plans for restoring critical services and operations after an incident.
- Change logs or records showing updates to recovery strategies and resilience plans based on lessons learned from exercises or actual incidents.
- Stakeholder feedback and review summaries that have led to updates in recovery strategies or resilience plans.
- Training session records for staff on updated recovery procedures and resilience measures.
- Audit reports or assessments that have identified areas for improvement in recovery strategies, leading to plan updates.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EEE-106: Recovery Objectives Critical Infrastructure Documentation

- Documentation of recovery objectives for critical infrastructure and how these align with business continuity goals.
- Critical infrastructure analysis reports that assess the resilience and recovery capabilities of essential systems.
- Records of alignment discussions or decisions between recovery objectives and business needs.
- Audit reports evaluating the alignment of recovery objectives with the criticality of infrastructure components.

EEE-107: Data Recovery and Information Flow Mapping Documentation

- Data recovery strategy documents that outline procedures for restoring lost or corrupted data.
- Information flow maps that illustrate how data moves through the organization, informing recovery planning.
- Test reports from data recovery exercises, demonstrating the ability to restore data in line with recovery strategies.
- Documentation of changes to data recovery strategies based on new business processes or technologies.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Training records for IT staff on data recovery procedures and information flow considerations.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

EEE-111: Disaster Recovery and Validation Program Documentation

- Disaster Recovery (DR) plans outlining specific recovery steps for Information Technology (IT) systems and data.
- Schedules and results from regular DR testing, ensuring plans are actionable and up-to-date.
- Change management records for DR plans, capturing updates and justifications.
- Records capturing lessons-learned from exercises and the updating of documentation and plans to reflect the improvements.
- Training and certification records for personnel on DR roles and procedures.
- Review reports assessing DR plan alignment with overall business recovery objectives and Business Impact Analyses (BIAs).

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GOVERN / Risk Management Strategy / Risk Management Objectives Agreement

GV.RM-01.01: Technology and cybersecurity risk management strategies and frameworks are approved by the governing authority (e.g., the Board or one of its committees) and incorporated into the overall business strategy and enterprise risk management framework.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #enterprise_risk_management | #metrics_and_reporting | #mission_and_strategy | #risk_management | #risk_oversight

Response Guidance:

The organization's technology and cybersecurity risk management strategies and frameworks should be a key consideration in all business strategies, practices, policies, and procedures. The technology and cybersecurity risk management strategies should align with long-term business strategies and the technologies to support these strategies. Management can support an enterprise information security program and enterprise risk management framework by setting a strong security culture that begins with board involvement and ongoing cybersecurity awareness training that is expected at all levels of management and staff.

Include information about the organization's technology and cybersecurity risk management strategies and frameworks. Document the approval of the strategies and frameworks by the Board (or one of its committees) and outline how they incorporate business strategy and links to the enterprise risk management framework. For example, the cybersecurity risk management framework should be part of the organization's overall enterprise risk management framework. Describe how that framework is established and executed for cybersecurity risk management.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-002: Board Governance and IT Oversight Documentation

- Board of Directors' charter and governance guidelines.
- Copies of presentations, reports, and minutes from board meetings and committees related to IT and cybersecurity.
- Records of decisions and actions taken regarding IT governance.
- Policy documents on roles and responsibilities of governance bodies.
- Compliance reports related to governance policies and practices.

EEE-003: Strategic Objectives and Planning Documents

- Documentation ot the organization's mission statement.
- Strategic plan outlining the organization's objectives and key results.
- Executive summaries of strategic goals related to IT and cybersecurity.
- Performance reports against strategic objectives.
- Communications from leadership on strategic direction and priorities.

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-005: Risk Appetite Tolerance, and Strategy Alignment Documents

- Risk appetite statements approved by the board or executive management.
- Risk tolerance levels defined for different categories of risk.
- Documentation on how risk appetite influences decision-making and strategy.
- Reports on risk exposures compared to the defined risk appetite.
- Updates or revisions to risk appetite and tolerance based on changing conditions.

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-031: Cybersecurity and Technology Officer Leadership Documentation

- Job descriptions and role profiles for the Cybersecurity Officer and Technology Officer, outlining responsibilities and qualifications.
- Strategic plans and objectives developed by the Cybersecurity Officer and Technology Officer, with documented board or executive approval.
- Records of security initiatives led by these officers, including project plans, status updates, and outcomes.
- Documentation of regular updates or briefings provided to the board and senior management by these officers.
- Evidence of the performance of 360-degree reviews of the Cybersecurity Officer and Technology Officer.
- Performance evaluations or reviews of the Cybersecurity Officer and Technology Officer, assessing their effectiveness and impact.

EEE-032: Technology and Cybersecurity Personnel Roles and Responsibilities Documentation

- Organizational charts and role matrices that clearly define the roles and responsibilities of technology and cybersecurity personnel.
- Training and certification records for staff, demonstrating qualifications and ongoing professional development.
- Policies and procedures that outline the expected contributions of personnel to cybersecurity initiatives.
- Evaluations of skill and resource level requirements against the current personnel complement.
- Incident response team rosters and contact information, indicating roles during security incidents.
- Performance reviews and goal-setting documents for technology and cybersecurity staff.

EEE-093: Risk Management Strategy and Framework Documentation

- Documentation of the organization's risk management strategy and framework, outlining risk identification, assessment, and mitigation processes.
- Records from risk management framework review sessions, including updates made to adapt to new risks or business changes.
- Risk registers or databases tracking identified risks, assessments, and mitigation actions over time.
- Stakeholder reports summarizing the state of risk management within the organization and strategic recommendations.
- External audit or consultant reviews of the risk management framework, providing independent assessments and suggestions for improvement.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-094: Technology and Cybersecurity Risk Appetite Documents

- Official statements or documents defining the organization's risk appetite specifically related to technology and cybersecurity.
- Board or executive committee meeting minutes discussing and approving the risk appetite statement.
- Guidelines for aligning IT and cybersecurity initiatives with the defined risk appetite.
- Reviews or assessments of projects and initiatives to ensure they are within the organization's technology and cybersecurity risk appetite.

GV.RM-01.02: Technology and cybersecurity risk management strategies and frameworks are informed by applicable international, national, and financial services industry standards and guidelines.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #compliance | #industry_standards | #risk_management

Response Guidance:

The organization should leverage industry security standards and guidelines in the management of technology and cybersecurity risks and gaps in controls and processes. Responses should include evidence that the technology and cyber risk strategies and frameworks are built upon applicable industry standards and guidelines. Additionally, responses should provide evidence of technology and cyber risk strategy and framework are reviewed and updated to incorporate changes within applicable industry standards and guidelines.

Industry recognized standards commonly include standards from: the National Institute of Standards and Technology (NIST); SysAdmin, Audit, Network, Security (SANS); the International Organization for Standardization (ISO); the Payment Card Industry (PCI); and ISACA's Control Objectives for Information and Related Technology (COBIT). The Financial Services Cyber Profile, now the CRI Profile, was developed using these frameworks as informative references and it could be a valuable resource for this purpose.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.
- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-007: Legal, Regulatory, and Compliance Management Documentation

- Compliance audit reports for relevant laws and regulations (e.g., GDPR, HIPAA).
- Documentation of legal advice received on cybersecurity matters, to include determinations of incident materiality.
- Records of regulatory filings and notices related to IT and cybersecurity.
- Updates to policies and procedures in response to legal and regulatory changes.
- Training records on legal and regulatory requirements for IT staff.

EEE-042: Emerging Technology Risk and Opportunity Assessment Documentation

- Strategic reports evaluating the risks and opportunities associated with adopting new or emerging technologies.
- Risk assessment templates and completed assessments for specific technologies under consideration.
- Minutes from meetings or workshops where emerging technologies and their implications were discussed.
- Records of participation in industry events or education related to emerging technologies and risk management.
- Innovation pipeline documents that track the evaluation and adoption process for new technologies.
- Case studies or pilot project reports on the implementation of emerging technologies.

EEE-093: Risk Management Strategy and Framework Documentation

- Documentation of the organization's risk management strategy and framework, outlining risk identification, assessment, and mitigation processes.
- Records from risk management framework review sessions, including updates made to adapt to new risks or business changes.
- Risk registers or databases tracking identified risks, assessments, and mitigation actions over time.
- Stakeholder reports summarizing the state of risk management within the organization and strategic recommendations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

- External audit or consultant reviews of the risk management framework, providing independent assessments and suggestions for improvement.

GV.RM-01.03: The organization has established, and maintains, technology and cybersecurity programs designed to protect the confidentiality, integrity and availability of its information and operational systems, commensurate with the organization's risk appetite and business needs.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #data_integrity | #data_protection | #mission_and_strategy | #program_transformation | #risk_appetite_/_tolerance | #risk_management | #system_integrity | #technology_availability | #improvements

Response Guidance:

Describe how the technology and cybersecurity programs are maintained, managed, and governed. Provide examples of how the programs assess and manage processes, activities, or systems, to ensure that they are operating effectively and work with all of the organization's business functions to understand and manage the risks. Describe the technology and cybersecurity programs performance measures and risk indicators (e.g., KRIs, KPIs, and KCIs), and how the program addresses inherent risk to the organization. Describe how the programs are reviewed and approved annually at the Board Risk Committee.

Describe how the organization strengthens the technology and cybersecurity capabilities in line with the organization's risk appetite and reducing the likelihood of a successful cyber-attack or service disruption. Provide examples of how programs align to industry recognized cyber frameworks and standards (e.g., the CRI Profile, NIST, ISO, FFIEC CAT, etc.)

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-005: Risk Appetite Tolerance, and Strategy Alignment Documents

- Risk appetite statements approved by the board or executive management.
- Risk tolerance levels defined for different categories of risk.
- Documentation on how risk appetite influences decision-making and strategy.
- Reports on risk exposures compared to the defined risk appetite.
- Updates or revisions to risk appetite and tolerance based on changing conditions.

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

EEE-039: Malware Protection and Incident Detection Documentation

- Anti-malware policies and procedures, including strategies for prevention, detection, and response.
- Logs from anti-malware solutions showing coverage, detection, and remediation of malicious software.
- Exception reports and tracking of malware detection failures and gaps.
- Incident response plans that include specific protocols for handling malware-related incidents.
- Post-incident analysis reports that evaluate the effectiveness of malware protection strategies.

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

EEE-093: Risk Management Strategy and Framework Documentation

- Documentation of the organization's risk management strategy and framework, outlining risk identification, assessment, and mitigation processes.
- Records from risk management framework review sessions, including updates made to adapt to new risks or business changes.
- Risk registers or databases tracking identified risks, assessments, and mitigation actions over time.
- Stakeholder reports summarizing the state of risk management within the organization and strategic recommendations.
- External audit or consultant reviews of the risk management framework, providing independent assessments and suggestions for improvement.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

GV.RM-01.04: Technology and cybersecurity risk management programs incorporate risk identification, measurement, monitoring, and reporting.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #enterprise_risk_management | #risk_management

Response Guidance:

The organization’s technology and cyber risk management programs should incorporate defined and structured processes to the likelihood and impact of threats and identify mitigating controls. The program should also identify inherent risk and measure, monitor, and report the effectiveness of controls and residual risk.

Describe how the technology and cyber risk management programs incorporate risk identification, measurement, monitoring, and reporting. Provide the organization’s enterprise risk management framework where there is an available risk and control library, how risk and control assessments are completed (identification of key risks and mitigating controls) and monitoring and reporting of such

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

risks. Include any additional organization-specific tools to measure technology and cyber risk reductions.

Examples of Effective Evidence:

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-046: Risk Assessment and Threat Analysis Documentation

- Standardized risk assessment templates.
- Completed assessments for relevant organizational assets and processes.
- Threat analysis reports that identify potential threats and their likelihood and impact on the organization.
- Documentation of risk assessment training for staff involved in the risk management process.
- Risk registers or databases that track identified risks and their mitigation status.
- Historical trend analysis of threats and incidents to inform future risk assessments.

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.
- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

EEE-050: Control Assessment and Testing Documentation

- Schedules and plans for regular assessments and testing of security controls to ensure they are functioning as intended.
- Results and reports from control assessments, including identified deficiencies and corrective actions taken.
- Documentation of testing methodologies and criteria used to evaluate the effectiveness of controls.
- Records of updates or changes to controls based on assessment findings.

EEE-053: Project Governance, Management, and Quality Assurance Documentation

- Project governance frameworks or charters that define roles, responsibilities, and decision-making processes.
- Stakeholder analysis documents and communication plans for engaging with project stakeholders.
- Project management plans that include quality control measures, checkpoints, risk mitigation strategies, and contingency planning.
- Risk assessment templates and completed assessments for technology projects, identifying potential delivery risks.
- Quality assurance policies and procedures for overseeing project deliverables and outcomes.
- Checklists and tools used for quality control during project execution.
- Meeting minutes and action items from project steering committees, governance boards, or risk management discussions within project teams, including actions taken to address identified risks.
- Records of project audits or reviews focused on quality aspects.
- Feedback and satisfaction surveys from stakeholders regarding project outcomes and engagement.
- Reports on project performance, governance effectiveness, and risk management effectiveness, including lessons learned.
- Training documentation for project managers and team members on quality management practices and risk assessment and management techniques.
- Post-project reviews or retrospectives that analyze risk management effectiveness and lessons learned.
- Documentation of project management standards, methodologies, and best practices adopted by the organization

EEE-054: Technology Service Performance and Support Monitoring Documentation

- Service level agreements (SLAs) and key performance indicators (KPIs) for technology services and support functions.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation for service catalogs, service support systems, or other mechanisms for end-users to request services.
- Monitoring dashboards or reports that track service performance against SLAs and KPIs.
- Records of service incidents, including response times, resolution details, and customer feedback.
- Procedures for managing and improving technology service performance.

EEE-068: Threat Monitoring and Detection Program Evaluation Documentation

- Documentation of the monitoring and detection strategies employed to identify potential security threats and vulnerabilities.
- Evaluation reports detailing the effectiveness of monitoring tools and detection mechanisms in identifying and mitigating risks.
- Training records for security personnel on the use of monitoring and detection technologies and techniques.
- Change logs demonstrating updates and improvements made to monitoring and detection capabilities.
- Incident case studies showcasing successful detection and response actions facilitated by the monitoring program.

EEE-081: Incident Analysis and Triage Process Documentation

- Documentation of standardized processes for analyzing and triaging security incidents, including criteria for categprization and prioritization.
- Logs and reports from incident management systems showing the application of triage processes in real incidents.
- After-action reviews or lessons learned documents from incidents, highlighting the effectiveness of analysis and triage procedures.
- Continuous improvement plans based on feedback and performance metrics from incident analysis activities.

EEE-087: Security Control and Process Improvement Documents

- Continuous improvement plans for security controls and processes, detailing objectives, actions, timelines, and responsible parties.
- Budget requests and justifications for improvement recommendations.
- Documentation of security control assessments, including findings and recommendations for enhancements.
- Change management records for updates to security processes and controls, including rationale and outcomes.
- Feedback collection mechanisms and reports from users and stakeholders on security controls, informing improvement plans.
- Performance metrics and monitoring reports that track the effectiveness of security controls and process improvements over time.

EEE-096: Incident Detection and Response Coordination Documentation

- Incident detection policies and procedures that define how potential security events are identified and analyzed.
- Coordination plans that outline roles and communication protocols for responding to incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Logs and reports from detection tools and systems, including details of incident analysis and response actions.
- Training and exercise records for response teams, demonstrating preparedness and coordination effectiveness.
- After-action reports and lessons learned from incident responses, used to improve future coordination.

GV.RM-01.05: The organization's technology, cybersecurity, resilience, and third-party risk management programs, policies, resources, and priorities are aligned and mutually supporting.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #dependency_management | #program_transformation | #resilience | #risk_management | #third_party_risk_management | #supply_chain_management

Response Guidance:

The organization should have a policies, standards, and procedures mutually support each other to address business requirements while maintaining security and resiliency. Responses should describe the policy development lifecycle. The lifecycle should include cross collaboration with other business functions to mutually support each program. Describe how resources are allocated to support the organizations business needs and across business functions.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.
- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Business continuity plan outlining procedures for maintaining service delivery during disruptions.
- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.
- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.
- Contingency plans detailing alternative service delivery methods.
- Training records for staff on resilience and continuity procedures and their roles during incidents.

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.
- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-059: Enterprise and Cyber Resilience Policy Documentation

- Official enterprise resilience strategy documents that outline the organization's approach to achieving and maintaining resilience.
- Cyber resilience policy documents that specify the measures and controls in place to protect against cyber threats.
- Board presentations and approvals related to the resilience strategy and cyber resilience policies.
- Reports from resilience assessments, including gap analyses and recommendations for improvement.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Risk management review reports that are presented to the board, including findings and recommendations.
- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.
- Training materials for board members on risk management principles and their oversight responsibilities.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

GOVERN / Risk Management Strategy / Risk Appetite & Risk Tolerance Statements

GV.RM-02.01: The governing authority (e.g., the Board or one of its committees) endorses and regularly reviews technology and cybersecurity risk appetite and is regularly informed about the status of, and material changes to, the organization's inherent risk profile.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #risk_appetite_/_tolerance | #risk_management | #risk_oversight | #roles_and_responsibilities | #threat_management

Response Guidance:

Risk appetite can be defined as a broad-based description of the desired level of risk that an entity will take in the pursuit of its mission. Risk appetite statements and risk tolerance metrics should describe systems and services that the organization may consider high-risk. Risk appetite statements should be decided by management after review, debate and informed determination based on business objectives and stakeholder expectations and not in isolation by any one person or department and the board. These statements should be further reviewed and approved by the board.

Responses should provide information and examples of technology and cyber risk appetite and risk tolerance, including the oversight, review, and approval processes. Include various board and committee information, organizational charts, roles, and responsibilities. Describe how the organization’s governing authority reviews technology and cyber risks and updates procedures based on identified threats. Describe the organization’s process and procedures for informing the governing body (e.g, the board or one of its committees) regarding the status of, and/or material changes to the inherent risk profile.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Organizations should demonstrate that there is a defined process to elevate the existence of a technology and cyber risks within the organization to management's attention should it exceed the maximum acceptable level outlined in the risk appetite statement. As such, organizations should include information on their company's cyber risk escalation process.

Examples of Effective Evidence:

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-005: Risk Appetite Tolerance, and Strategy Alignment Documents

- Risk appetite statements approved by the board or executive management.
- Risk tolerance levels defined for different categories of risk.
- Documentation on how risk appetite influences decision-making and strategy.
- Reports on risk exposures compared to the defined risk appetite.
- Updates or revisions to risk appetite and tolerance based on changing conditions.

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.
- Risk management review reports that are presented to the board, including findings and recommendations.
- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.
- Training materials for board members on risk management principles and their oversight responsibilities.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-093: Risk Management Strategy and Framework Documentation

- Documentation of the organization's risk management strategy and framework, outlining risk identification, assessment, and mitigation processes.
- Records from risk management framework review sessions, including updates made to adapt to new risks or business changes.
- Risk registers or databases tracking identified risks, assessments, and mitigation actions over time.
- Stakeholder reports summarizing the state of risk management within the organization and strategic recommendations.
- External audit or consultant reviews of the risk management framework, providing independent assessments and suggestions for improvement.

EEE-094: Technology and Cybersecurity Risk Appetite Documents

- Official statements or documents defining the organization's risk appetite specifically related to technology and cybersecurity.
- Board or executive committee meeting minutes discussing and approving the risk appetite statement.
- Guidelines for aligning IT and cybersecurity initiatives with the defined risk appetite.
- Reviews or assessments of projects and initiatives to ensure they are within the organization's technology and cybersecurity risk appetite.

GV.RM-02.02: The organization has established statements of technology and cybersecurity risk tolerance consistent with its risk appetite, and has integrated them into technology, cybersecurity, operational, and enterprise risk management practices.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #enterprise_risk_management | #risk_appetite_/_tolerance | #risk_management

Response Guidance:

Provide information on the organization’s cyber risk tolerance and risk appetite statement including details on inherent and residual risk levels. Provide evidence of linkage between KRIs and risk appetite/risk tolerance. Describe the process of defining and updating the risk tolerance statement, including the types of reviews and approvals that take place.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.
- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-005: Risk Appetite Tolerance, and Strategy Alignment Documents

- Risk appetite statements approved by the board or executive management.
- Risk tolerance levels defined for different categories of risk.
- Documentation on how risk appetite influences decision-making and strategy.
- Reports on risk exposures compared to the defined risk appetite.
- Updates or revisions to risk appetite and tolerance based on changing conditions.

EEE-093: Risk Management Strategy and Framework Documentation

- Documentation of the organization's risk management strategy and framework, outlining risk identification, assessment, and mitigation processes.
- Records from risk management framework review sessions, including updates made to adapt to new risks or business changes.
- Risk registers or databases tracking identified risks, assessments, and mitigation actions over time.
- Stakeholder reports summarizing the state of risk management within the organization and strategic recommendations.
- External audit or consultant reviews of the risk management framework, providing independent assessments and suggestions for improvement.

EEE-094: Technology and Cybersecurity Risk Appetite Documents

- Official statements or documents defining the organization's risk appetite specifically related to technology and cybersecurity.
- Board or executive committee meeting minutes discussing and approving the risk appetite statement.
- Guidelines for aligning IT and cybersecurity initiatives with the defined risk appetite.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Reviews or assessments of projects and initiatives to ensure they are within the organization's technology and cybersecurity risk appetite.

EEE-104: Risk Tolerance and Management Practice Integration Documentation

- Documentation of the organization's risk tolerance levels and how these are integrated into risk management practices.
- Records of risk assessments that consider the organization's risk tolerance when determining mitigation strategies.
- Reports to management and the board on risk exposures in relation to the defined risk tolerance.
- Reviews of risk management practices to ensure they remain aligned with the organization's risk tolerance.

GV.RM-02.03: Determination of the organization's risk appetite and tolerance includes consideration of the organization's stakeholder obligations, role in critical infrastructure, and sector-specific risk analysis.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #business_impact_analysis | #critical_infrastructure | #enterprise_risk_management | #risk_appetite_/_tolerance | #risk_management | #roles_and_responsibilities

Response Guidance:

When establishing risk appetite and risk tolerance, the organization's management should consider its role as a critical infrastructure organization and calibrate the risk appetite and tolerance, if applicable, relative to that role. Provide information in support of the risk appetite and risk tolerance being informed by the organization's role in critical infrastructure.

Describe the disposition of the risk appetite and risk tolerance, in addition to cycle of review of risk appetite statement and aspects that support the risk appetite and tolerance. The evaluation of risk appetite and tolerance should include the organization's role within the sector and their obligations to stakeholders, clients, and customers. Provide information on how the organization coordinates with various financial services bodies, such as the ARC and FS-ISAC, and how the organization responds to risk information received by these bodies.

Examples of Effective Evidence:

EEE-005: Risk Appetite Tolerance, and Strategy Alignment Documents

- Risk appetite statements approved by the board or executive management.
- Risk tolerance levels defined for different categories of risk.
- Documentation on how risk appetite influences decision-making and strategy.
- Reports on risk exposures compared to the defined risk appetite.
- Updates or revisions to risk appetite and tolerance based on changing conditions.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-007: Legal, Regulatory, and Compliance Management Documentation

- Compliance audit reports for relevant laws and regulations (e.g., GDPR, HIPAA).
- Documentation of legal advice received on cybersecurity matters, to include determinations of incident materiality.
- Records of regulatory filings and notices related to IT and cybersecurity.
- Updates to policies and procedures in response to legal and regulatory changes.
- Training records on legal and regulatory requirements for IT staff.

EEE-105: Stakeholder Obligation Compliance and Sector-Specific Risk Analysis Documents

- Policies and procedures that address stakeholder obligations and sector-specific risks.
- Sector-specific risk analysis reports that identify unique risks and compliance requirements.
- Documentation of compliance audits or assessments, including findings and actions taken to address gaps.
- Agreements or contracts with stakeholders that include compliance with sector-specific obligations and standards.

EEE-106: Recovery Objectives Critical Infrastructure Documentation

- Documentation of recovery objectives for critical infrastructure and how these align with business continuity goals.
- Critical infrastructure analysis reports that assess the resilience and recovery capabilities of essential systems.
- Records of alignment discussions or decisions between recovery objectives and business needs.
- Audit reports evaluating the alignment of recovery objectives with the criticality of infrastructure components.

GOVERN / Risk Management Strategy / Enterprise Risk Integration

GV.RM-03.01: Technology and cybersecurity risk management frameworks and programs are integrated into the enterprise risk management framework.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #enterprise_risk_management | #risk_management

Response Guidance:

The technology and cyber risk management framework and threat intelligence processes should be integrated with the enterprise risk management process to ensure the risk of relevant threats is analyzed relative to enterprise level impacts. Enterprise risk management objectives and actions encompass technology and cybersecurity risk mitigation and acceptance decisions. These decisions align with overall risk tolerance and enable, rather than limit or prohibit, business objectives.

Describe how the organization integrates the technology and cyber risk management frameworks into the enterprise risk management framework. Provide information on how the organization follows an enterprise risk management framework and operational risk management framework for the

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

management of risks using a three lines of defense model. For example, describe how the First Line of Defense (1LoD) implements controls and the Second Line of Defense (2LoD) reviews and challenges the 1LoD.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.
- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-059: Enterprise and Cyber Resilience Policy Documentation

- Official enterprise resilience strategy documents that outline the organization's approach to achieving and maintaining resilience.
- Cyber resilience policy documents that specify the measures and controls in place to protect against cyber threats.
- Board presentations and approvals related to the resilience strategy and cyber resilience policies.
- Reports from resilience assessments, including gap analyses and recommendations for improvement.

EEE-066: Segregation of Duties in Risk Management Documentation

- Policies and procedures that establish segregation of duties within risk management activities to prevent conflicts of interest and fraud.
- Flowcharts or diagrams that illustrate the separation of roles and responsibilities in risk-related processes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Internal control reports that verify the effectiveness of segregation of duties in mitigating risks.
- Records of changes to duties or responsibilities to maintain proper segregation as the organization evolves.

EEE-093: Risk Management Strategy and Framework Documentation

- Documentation of the organization's risk management strategy and framework, outlining risk identification, assessment, and mitigation processes.
- Records from risk management framework review sessions, including updates made to adapt to new risks or business changes.
- Risk registers or databases tracking identified risks, assessments, and mitigation actions over time.
- Stakeholder reports summarizing the state of risk management within the organization and strategic recommendations.
- External audit or consultant reviews of the risk management framework, providing independent assessments and suggestions for improvement.

GV.RM-03.02: The organization's business continuity and resilience strategy and program align with and support the overall enterprise risk management framework.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #resilience | #risk_management

Response Guidance:

Cyber threats and disruptions impacting an organization can proliferate to the systems of other organizations due to the interconnectivity among systems. The organization’s management should be actively involved in monitoring cybersecurity risks that the organization may pose to other critical infrastructures, as well as dependencies on those infrastructures. Describe how the cyber resilience strategy and program are aligned with the organization's enterprise-wide cyber risk management strategy. Describe how the strategy and program addresses enterprise-level needs and the risks that the organization may present to other critical infrastructure sectors and the risk that the organization may present to other organizations in the financial sector.

Examples of Effective Evidence:

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.
- Business continuity plan outlining procedures for maintaining service delivery during disruptions.
- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.
- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Contingency plans detailing alternative service delivery methods.
- Training records for staff on resilience and continuity procedures and their roles during incidents.

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.
- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-016: Recovery Objectives and Strategic Alignment Documentation

- Tools and templates used for formulating recovery strategies that support business objectives.
- A matrix aligning recovery time and point objectives with business priorities.
- Documentation from strategic planning sessions focused on recovery objectives.
- Signed approvals from management endorsing the proposed recovery strategies.
- Periodic review reports assessing the alignment of recovery objectives with business needs.

EEE-058: Resilience Mechanism Validation and Feedback Documentation

- Plans and procedures for implementing resilience mechanisms across IT systems and business processes.
- Business- and associated system-level requirements for resilience.
- Architecture and design documentation detailing resilience deisgn factors and considerations.
- Schedules and reports from testing and exercises designed to validate the effectiveness of resilience mechanisms.
- Change management documentation related to the enhancement of resilience mechanisms.
- Lessons learned and improvement plans derived from resilience testing activities.
- Stakeholder feedback on the organization's resilience capabilities, gathered through surveys or interviews.

EEE-059: Enterprise and Cyber Resilience Policy Documentation

- Official enterprise resilience strategy documents that outline the organization's approach to achieving and maintaining resilience.
- Cyber resilience policy documents that specify the measures and controls in place to protect against cyber threats.
- Board presentations and approvals related to the resilience strategy and cyber resilience policies.
- Reports from resilience assessments, including gap analyses and recommendations for improvement.

EEE-078: Resilience Testing and Infrastructure Redundancy Documentation

- Documentation of resilience testing plans and procedures, including objectives, scenarios, and expected outcomes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Test reports summarizing the results of resilience testing exercises, highlighting strengths and areas for improvement.
- Infrastructure redundancy designs and implementation records, showing failover capabilities and backup systems.
- Change management records documenting updates or enhancements made to improve infrastructure redundancy.
- Stakeholder feedback on the organization's resilience and redundancy capabilities, gathered after testing or actual events.

EEE-091: Enterprise Resilience Strategy Documentation

- Documentation of the enterprise resilience strategy, outlining objectives, programs, and initiatives designed to enhance organizational resilience.
- Records of resilience program meetings, including strategic decisions, program updates, and progress tracking.
- Training and awareness materials developed to promote resilience across the organization.
- Performance metrics and reports evaluating the effectiveness of resilience programs and initiatives.
- Feedback from internal and external stakeholders on the organization's resilience capabilities and areas for improvement.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EEE-111: Disaster Recovery and Validation Program Documentation

- Disaster Recovery (DR) plans outlining specific recovery steps for Information Technology (IT) systems and data.
- Schedules and results from regular DR testing, ensuring plans are actionable and up-to-date.
- Change management records for DR plans, capturing updates and justifications.
- Records capturing lessons-learned from exercises and the updating of documentation and plans to reflect the improvements.
- Training and certification records for personnel on DR roles and procedures.
- Review reports assessing DR plan alignment with overall business recovery objectives and Business Impact Analyses (BIAs).

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GV.RM-03.03: Technology and cybersecurity risk management and risk assessment processes are consistent with the organization's enterprise risk management policies, procedures, and methodologies and include criteria for the evaluation and categorization of enterprise-specific risks and threats.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #enterprise_risk_management | #policy_management | #review_assessment_and_testing | #risk_management

Response Guidance:

The technology and cybersecurity risk management and risk assessments should identity internal and external risks, threats, and vulnerabilities that could result in unauthorized disclosure, misuse, alteration, or destruction of information systems supporting core business lines such as customer information or other sensitive data. The risk assessments should identify the likelihood and potential damage of these threats, and validate whether policies, procedures, and controls in place are appropriately mitigating risks.

Describe how the technology and cybersecurity risk management and risk assessments processes are aligned with the organization's policies, procedures, and methodologies. Highlight the criteria used for the evaluation and categorization of technology and cybersecurity risks within the context of enterprise-level risks, and threats, and vulnerabilities.

Examples of Effective Evidence:

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-046: Risk Assessment and Threat Analysis Documentation

- Standardized risk assessment templates.
- Completed assessments for relevant organizational assets and processes.
- Threat analysis reports that identify potential threats and their likelihood and impact on the organization.
- Documentation of risk assessment training for staff involved in the risk management process.
- Risk registers or databases that track identified risks and their mitigation status.
- Historical trend analysis of threats and incidents to inform future risk assessments.

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.
- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

EEE-050: Control Assessment and Testing Documentation

- Schedules and plans for regular assessments and testing of security controls to ensure they are functioning as intended.
- Results and reports from control assessments, including identified deficiencies and corrective actions taken.
- Documentation of testing methodologies and criteria used to evaluate the effectiveness of controls.
- Records of updates or changes to controls based on assessment findings.

EEE-051: Risk Metrics and Performance Indicator Documentation

- Key performance indicators (KPIs) and risk metrics used to measure the effectiveness of the organization's risk management program.
- Dashboards or reports that track and display collected performance indicators and risk metrics.
- Documentation of the process for collecting, analyzing, and reporting on KPIs and risk metrics.
- Historical data and trend analysis used to inform risk management decisions and strategies.
- Records of management reviews or meetings where performance indicators and risk metrics are discussed and used to drive decision making or improvements.

EEE-081: Incident Analysis and Triage Process Documentation

- Documentation of standardized processes for analyzing and triaging security incidents, including criteria for categprization and prioritization.
- Logs and reports from incident management systems showing the application of triage processes in real incidents.
- After-action reviews or lessons learned documents from incidents, highlighting the effectiveness of analysis and triage procedures.
- Continuous improvement plans based on feedback and performance metrics from incident analysis activities.

EEE-096: Incident Detection and Response Coordination Documentation

- Incident detection policies and procedures that define how potential security events are identified and analyzed.
- Coordination plans that outline roles and communication protocols for responding to incidents.
- Logs and reports from detection tools and systems, including details of incident analysis and response actions.
- Training and exercise records for response teams, demonstrating preparedness and coordination effectiveness.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- After-action reports and lessons learned from incident responses, used to improve future coordination.

GV.RM-03.04: Technology and cybersecurity risk management considerations are integrated into daily operations, cultural norms, management discussions, and management decision-making, and are tailored to address enterprise-specific risks (both internal and external).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #enterprise_risk_management | #risk_management

Response Guidance:

The consideration of technology and cyber risks should be embedded in strategic and tactical planning activities and not managed as a downstream or separate function. The organization should implement formal processes that ensures technology and cyber risks are considered across business units within the organization and that a risk-aware culture is promoted at all levels of management.

Describe and provide evidence supporting the technology and cyber risk management program linkages to the operational risk management framework. Provide information on the three lines of defense and the responsibility of each line to evaluate and manage identified risks. Describe how industry standards or frameworks being used (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), etc.) are aligned with the operational risk management framework.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.
- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-006: Cybersecurity, Culture, and Training Record Documents

- Employee cybersecurity awareness survey results.
- Training attendance logs for cybersecurity and IT policy courses.
- Assessments of organizational culture regarding security practices.
- Feedback and improvement reports following culture assessments.
- Records of cultural change initiatives related to cybersecurity.

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.
- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

EEE-041: Data Governance and Retention Policy Documentation

- Data governance framework documents that outline roles, responsibilities, and processes for managing organizational data.
- Data retention schedules and policies specifying how long different types of data should be kept and the procedures for data disposal.
- Audit reports demonstrating compliance with data management and retention policies.
- Documentation of automated and manual processes used to implement data retention requirements.
- Training records for staff on data governance practices and data handling procedures.
- Documentation of data classification schemes used to manage data based on its sensitivity and importance.

EEE-072: Cybersecurity Training for Leadership Documentation

- Agendas and materials from cybersecurity training sessions specifically designed for the organization's governing body and senior management.
- Records of attendance and participation in cybersecurity training by board members and senior executives.
- Evaluations or assessments of cybersecurity knowledge before and after training sessions.
- Documentation of cybersecurity briefings or updates provided to the governing body and senior management on a regular basis.
- Feedback from senior leaders on the relevance and effectiveness of the cybersecurity training they received.

EEE-073: Governance Access to Cybersecurity Expertise Documents

- Contracts or agreements with external cybersecurity experts or advisory firms engaged to support governance activities.
- Records of cybersecurity expert consultations or briefings provided to the governing body or committees.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of in-house cybersecurity expertise available to the governing body, including staff qualifications and roles.
- Minutes from governance meetings where cybersecurity experts provided input or guidance on decision-making.
- Evaluations of the cybersecurity expertise utilized by the governing body, assessing its impact on governance decisions.

GOVERN / Risk Management Strategy / Risk Response Strategic Direction

GV.RM-04.01: The governing authority (e.g., the Board or one of its committees) and senior management provide guidance, direction, and credible challenge in the design and implementation of risk management strategies, assessment of identified risks against risk appetite and risk tolerance, and in the selection of risk treatment approaches.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #metrics_and_reporting | #review_assessment_and_testing | #risk_appetite_/_tolerance | #risk_management | #risk_oversight | #roles_and_responsibilities

Response Guidance:

Enterprise risk management strategies, assessments, and risk treatment approaches encompass technology and cybersecurity. Describe how the governing authority (e.g., the Board or one of its committees) and senior management provide guidance, direction, and credible challenge in the design and implementation of risk management strategies, assessment of identified risks against risk appetite and risk tolerance, and in the selection of risk treatment approaches. Provide examples of the governing authority reviewing, providing guidance, and approving the risk management strategies, assessments, and risk treatment approaches, including documentation and evidence of review of credible challenge.

Examples of Effective Evidence:

EEE-005: Risk Appetite Tolerance, and Strategy Alignment Documents

- Risk appetite statements approved by the board or executive management.
- Risk tolerance levels defined for different categories of risk.
- Documentation on how risk appetite influences decision-making and strategy.
- Reports on risk exposures compared to the defined risk appetite.
- Updates or revisions to risk appetite and tolerance based on changing conditions.

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-031: Cybersecurity and Technology Officer Leadership Documentation

- Job descriptions and role profiles for the Cybersecurity Officer and Technology Officer, outlining responsibilities and qualifications.
- Strategic plans and objectives developed by the Cybersecurity Officer and Technology Officer, with documented board or executive approval.
- Records of security initiatives led by these officers, including project plans, status updates, and outcomes.
- Documentation of regular updates or briefings provided to the board and senior management by these officers.
- Evidence of the performance of 360-degree reviews of the Cybersecurity Officer and Technology Officer.
- Performance evaluations or reviews of the Cybersecurity Officer and Technology Officer, assessing their effectiveness and impact.

EEE-032: Technology and Cybersecurity Personnel Roles and Responsibilities Documentation

- Organizational charts and role matrices that clearly define the roles and responsibilities of technology and cybersecurity personnel.
- Training and certification records for staff, demonstrating qualifications and ongoing professional development.
- Policies and procedures that outline the expected contributions of personnel to cybersecurity initiatives.
- Evaluations of skill and resource level requirements against the current personnel complement.
- Incident response team rosters and contact information, indicating roles during security incidents.
- Performance reviews and goal-setting documents for technology and cybersecurity staff.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.
- Risk management review reports that are presented to the board, including findings and recommendations.
- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.
- Training materials for board members on risk management principles and their oversight responsibilities.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-093: Risk Management Strategy and Framework Documentation

- Documentation of the organization's risk management strategy and framework, outlining risk identification, assessment, and mitigation processes.
- Records from risk management framework review sessions, including updates made to adapt to new risks or business changes.
- Risk registers or databases tracking identified risks, assessments, and mitigation actions over time.
- Stakeholder reports summarizing the state of risk management within the organization and strategic recommendations.
- External audit or consultant reviews of the risk management framework, providing independent assessments and suggestions for improvement.

EEE-094: Technology and Cybersecurity Risk Appetite Documents

- Official statements or documents defining the organization's risk appetite specifically related to technology and cybersecurity.
- Board or executive committee meeting minutes discussing and approving the risk appetite statement.
- Guidelines for aligning IT and cybersecurity initiatives with the defined risk appetite.
- Reviews or assessments of projects and initiatives to ensure they are within the organization's technology and cybersecurity risk appetite.

EEE-104: Risk Tolerance and Management Practice Integration Documentation

- Documentation of the organization's risk tolerance levels and how these are integrated into risk management practices.
- Records of risk assessments that consider the organization's risk tolerance when determining mitigation strategies.
- Reports to management and the board on risk exposures in relation to the defined risk tolerance.
- Reviews of risk management practices to ensure they remain aligned with the organization's risk tolerance.

GOVERN / Risk Management Strategy / Lines of Communication

GV.RM-05.01: The organization has a process for monitoring its technology, cybersecurity, and third-party risks, including escalating those risks that exceed risk appetite to management and identifying risks with the potential to impact multiple operating units.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #risk_appetite_/_tolerance | #risk_management | #third_party_risk_management | #supply_chain_management

Response Guidance:

When technology, cyber, and/or third-party risks that exist within the organization exceeds the risk appetite, there should be a defined process to elevate this to management's attention. This process

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

should be understood by management and employees on what steps need to be taken to identify risks and the appropriate methods and channels to escalate potential issues to appropriate management and stakeholders.

Responses should include a description of the processes in place to identify, monitor, report, and escalate technology, cyber, and third-party risks. Describe how identified risks are rated, and for those that exceed tolerance, how are they escalated.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.
- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.
- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-068: Threat Monitoring and Detection Program Evaluation Documentation

- Documentation of the monitoring and detection strategies employed to identify potential security threats and vulnerabilities.
- Evaluation reports detailing the effectiveness of monitoring tools and detection mechanisms in identifying and mitigating risks.
- Training records for security personnel on the use of monitoring and detection technologies and techniques.
- Change logs demonstrating updates and improvements made to monitoring and detection capabilities.
- Incident case studies showcasing successful detection and response actions facilitated by the monitoring program.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

EEE-102: Vulnerability Disclosure Management Documentation

- Vulnerability disclosure policies that define how external reports of potential vulnerabilities are managed and addressed.
- Documentation of vulnerability disclosures received, including the organization's response and remediation efforts.
- Communication records with security researchers or reporting parties regarding vulnerability disclosures.
- Reports summarizing the outcomes of vulnerability disclosures and the effectiveness of the response process.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

GV.RM-05.02: The organization establishes minimum requirements for its third-parties that include how the organizations will communicate and coordinate in times of emergency, including:

1) Joint maintenance of contingency plans;

2) Responsibilities for responding to incidents, including forensic investigations;

3) Planning and testing strategies that address severe events in order to identify single points of failure that would cause wide-scale disruption; and

4) Incorporating the potential impact of an incident into their BCM process and ensure resilience capabilities are in place.

Subject Tags: #contract_management | #dependency_management | #third_party_risk_management | #supply_chain_management

Response Guidance:

As referenced in EX.CN-02.01, the organization has documented minimum cybersecurity requirements for third parties. Describe how minimum cybersecurity requirements for critical third parties include how the organization and its suppliers and partners will communicate and coordinate in times of emergency. Provide detail for each of the four areas highlighted in the full Diagnostic Statement. The organization's incident response program should address notification and communication with third parties regarding incidents at the third party that might impact the organization. Similarly, contracts with third parties should stipulate incident reporting requirements to ensure there are clearly documented processes and accountability for communicating and coordinating during times of emergencies.

Examples of Effective Evidence:

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.
- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-020: Vendor Contingency and Transition Planning Documents

- Contingency plans for transitioning services in case of vendor failure, including timelines and responsibilities.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Checklists for evaluating vendor contingency and recovery capabilities during the selection process.
- Documentation of transition exercises or drills conducted to test the effectiveness of contingency plans.
- Vendor exit strategy documents that outline procedures for terminating relationships while maintaining operational continuity.
- Records of vendor performance issues that triggered contingency or transition plans.

EEE-021: Third-Party Cybersecurity and Continuity Assessment Documentation

- Reports from cybersecurity assessments conducted on third-party vendors, including findings and recommendations.
- Third-party business continuity plans that detail recovery strategies and objectives relevant to services provided (or records of plan reviews).
- Agreements with third parties that include requirements for cybersecurity measures and business continuity planning.
- Documentation of joint business continuity exercises with critical vendors, including outcomes and improvements.
- Vendor cybersecurity certification records, verifying adherence to industry standards and best practices.

EEE-025: Vendor Contingency and Risk Mitigation Documentation

- Contingency plans that outline alternative solutions in case of vendor failure or service disruption.
- Risk assessments that identify potential points of failure with vendors and corresponding contingency options.
- Documentation of the evaluation and selection process for alternative vendors or solutions.
- Communication plans for engaging with alternative vendors during a contingency event.
- Test results from contingency plan exercises, demonstrating the viability of alternative solutions.

EEE-026: Third-Party Termination and Decommissioning Documentation

- Termination procedures and checklists that outline the steps for ending a relationship with a third party.
- Documentation of data retrieval or transfer processes upon termination of a third-party contract.
- Records of final account settlements and confirmations of service discontinuation.
- Technical closure reports that confirm the secure decommissioning of third-party services and systems.
- Exit interview records or final performance reviews with the third party, capturing lessons learned and final assessments.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

GOVERN / Risk Management Strategy / Standardized Risk Management Method

GV.RM-06.01: Technology and cybersecurity risk management and risk assessment processes and methodologies are documented and regularly reviewed and updated to address changes in the risk profile and risk appetite, the evolving threat environment, and new technologies, products, services, and interdependencies.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #enterprise_risk_management | #review_assessment_and_testing | #risk_appetite_/_tolerance | #risk_management | #threat_management

Response Guidance:

Technology and cybersecurity-related risks should be identified, reviewed, and analyzed as part of the organization's risk management processes. New products and services, as well as outsourced relationships, have the potential of introducing new or expanding existing technology and cybersecurity risks. Such risks should be evaluated to determine whether appropriate risk management processes are in place. On a regular basis, senior management should review and update risk management standards, practices, and procedures to be reflective of new technologies, products, services, and interdependencies (e.g., AI and quantum risks, cloud, and cloud third parties).

In addition, the threat environment is highly dynamic and prominent threats can necessitate revisiting these technology and cybersecurity risk management and risk assessments. Risk assessments should be updated with the most current information regarding widely known risks and risk management practices to assist management and the board in making informed decisions.

Provide evidence that the technology and cyber risk assessment processes and methodologies are documented and updated regularly. Demonstrate how risks are routinely addressed through management reporting of current and/or top and emerging risks within the organization to the Board and/or relevant committee (e.g., Board Risk Committee). Provide evidence that a technology and cybersecurity risk update is routinely provided by management to the Board Risk Committee.

Examples of Effective Evidence:

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

EEE-046: Risk Assessment and Threat Analysis Documentation

- Standardized risk assessment templates.
- Completed assessments for relevant organizational assets and processes.
- Threat analysis reports that identify potential threats and their likelihood and impact on the organization.
- Documentation of risk assessment training for staff involved in the risk management process.
- Risk registers or databases that track identified risks and their mitigation status.
- Historical trend analysis of threats and incidents to inform future risk assessments.

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.
- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.
- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

EEE-050: Control Assessment and Testing Documentation

- Schedules and plans for regular assessments and testing of security controls to ensure they are functioning as intended.
- Results and reports from control assessments, including identified deficiencies and corrective actions taken.
- Documentation of testing methodologies and criteria used to evaluate the effectiveness of controls.
- Records of updates or changes to controls based on assessment findings.

EEE-093: Risk Management Strategy and Framework Documentation

- Documentation of the organization's risk management strategy and framework, outlining risk identification, assessment, and mitigation processes.
- Records from risk management framework review sessions, including updates made to adapt to new risks or business changes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Risk registers or databases tracking identified risks, assessments, and mitigation actions over time.
- Stakeholder reports summarizing the state of risk management within the organization and strategic recommendations.
- External audit or consultant reviews of the risk management framework, providing independent assessments and suggestions for improvement.

GOVERN / Risk Management Strategy / Strategic Opportunities

GV.RM-07.01: The organization has mechanisms in place to ensure that strategies, initiatives, opportunities, and emerging technologies (e.g., artificial intelligence, quantum computing, etc.) are evaluated both in terms of risks and uncertainties that are potentially detrimental to the organization, as well as potentially advantageous to the organization (i.e., positive risks).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #emerging_technologies | #mission_and_strategy | #risk_management | #threat_management

Response Guidance:

As technologies, products, and services evolve the organization should understand the inherent risks and benefits before adoption. The review and assessment of the potentially detrimental risks against the advantageous benefits (i.e., positive risks) should be considered when evaluating, designing and implementing new technologies, strategies, and initiatives.

Provide evidence of risk management activities identifying and evaluating the inherent risk of new and existing technologies, initiatives, and potential opportunities. Describe the processes to identify the positive risks that may outweigh the detrimental risks. Describe how analysis determines how technology and cybersecurity activities will be implemented and safeguarded.

Examples of Effective Evidence:

EEE-042: Emerging Technology Risk and Opportunity Assessment Documentation

- Strategic reports evaluating the risks and opportunities associated with adopting new or emerging technologies.
- Risk assessment templates and completed assessments for specific technologies under consideration.
- Minutes from meetings or workshops where emerging technologies and their implications were discussed.
- Records of participation in industry events or education related to emerging technologies and risk management.
- Innovation pipeline documents that track the evaluation and adoption process for new technologies.
- Case studies or pilot project reports on the implementation of emerging technologies.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-053: Project Governance, Management, and Quality Assurance Documentation

- Project governance frameworks or charters that define roles, responsibilities, and decision-making processes.
- Stakeholder analysis documents and communication plans for engaging with project stakeholders.
- Project management plans that include quality control measures, checkpoints, risk mitigation strategies, and contingency planning.
- Risk assessment templates and completed assessments for technology projects, identifying potential delivery risks.
- Quality assurance policies and procedures for overseeing project deliverables and outcomes.
- Checklists and tools used for quality control during project execution.
- Meeting minutes and action items from project steering committees, governance boards, or risk management discussions within project teams, including actions taken to address identified risks.
- Records of project audits or reviews focused on quality aspects.
- Feedback and satisfaction surveys from stakeholders regarding project outcomes and engagement.
- Reports on project performance, governance effectiveness, and risk management effectiveness, including lessons learned.
- Training documentation for project managers and team members on quality management practices and risk assessment and management techniques.
- Post-project reviews or retrospectives that analyze risk management effectiveness and lessons learned.
- Documentation of project management standards, methodologies, and best practices adopted by the organization

EEE-090: Security and Resilience Design Standards Documents

- Official documents outlining security and resilience architectural and design standards that all technology projects and initiatives must adhere to.
- Checklists and templates used during the design phase of projects to ensure compliance with security and resilience standards.
- Records of design review sessions where security and resilience considerations were evaluated and enforced.
- Case studies or examples of projects that successfully implemented these design standards.
- Audit or review reports assessing adherence to security and resilience design standards across projects.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Application Security standard, policies, procedures

GOVERN / Risk Management Strategy / Technology Assimilation & Implementations

GV.RM-08.01: Technology and cybersecurity risk management frameworks are applied to, and are adapted as needed by, the organization's innovations in technology use and adoption of emerging technologies.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #emerging_technologies | #mission_and_strategy | #risk_management | #threat_management

Response Guidance:

Describe the continuous analysis of the threat environment and attack vectors for potential outcomes and how this contributes to ongoing investment in emerging technologies to defend against these threats. Provide information on how security is considered throughout project and technology implementation (e.g., risk assessments during procurement planning).

Describe how technology and cybersecurity activities, such as appropriate risk assessment, business impact, security evaluations, and mitigating controls, are considered before the organization integrates new technologies, and how cybersecurity is considered as part of any approval process for new projects. Provide information on how analysis data links to the various risk programs, updating of policies, and standards. Describe how risk management frameworks are adapted to deal with emerging technologies (e.g., AI and cloud).

Examples of Effective Evidence:

EEE-023: Third Party Technology Security Assessment and Compliance Documents

- Assessment reports for third party software and technology, including security reviews and compliance checks.
- Documentation of the criteria and standards used for technology assessments.
- Change logs for external software, indicating how updates and patches are managed.
- Reports from third party vulnerability and security evaluation scanning services
- Vendor security certifications or attestations, such as SOC 2 reports or ISO certifications.
- Records of security testing, such as penetration tests or vulnerability scans, performed on third-party technologies.

EEE-042: Emerging Technology Risk and Opportunity Assessment Documentation

- Strategic reports evaluating the risks and opportunities associated with adopting new or emerging technologies.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Risk assessment templates and completed assessments for specific technologies under consideration.
- Minutes from meetings or workshops where emerging technologies and their implications were discussed.
- Records of participation in industry events or education related to emerging technologies and risk management.
- Innovation pipeline documents that track the evaluation and adoption process for new technologies.
- Case studies or pilot project reports on the implementation of emerging technologies.

EEE-052: Technology Architecture and Design Documentation

- Architecture diagrams and design documents that detail the structure and components of the organization's technology systems, including networks, systems, and applications.
- Records of architecture review board meetings, including decisions on technology design, changes, and rationales for architectural changes.
- Documentation of technology standards, design patterns, and best practices adopted in system design.
- Change history logs and version control records for architectural designs and documents, showing evolution and updates over time.
- Compliance certificates, reports, and assessments verifying that designs and architecture meet relevant industry standards and regulatory requirements.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

GV.RM-08.02: Technology and cybersecurity risk management frameworks are applied to all technology projects and procurements to ensure that security requirements (e.g., data confidentiality, access control, event logging, etc.) are addressed consistently from project onset.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #change_management | #review_assessment_and_testing | #risk_management | #security_baselines

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Any time new technologies, products, services, connections or relationships are added to the existing business environment, management should be responsible for assessing potential risk elevation, if any, and the need for additional mitigating controls.

Provide information on how the organization applies the cyber risk management framework to all technology projects. Describe how all projects follow a documented framework and how the framework assists project managers, project teams, and security teams to establish the documentation and governance required for the project.

Examples of Effective Evidence:

EEE-023: Third Party Technology Security Assessment and Compliance Documents

- Assessment reports for third party software and technology, including security reviews and compliance checks.
- Documentation of the criteria and standards used for technology assessments.
- Change logs for external software, indicating how updates and patches are managed.
- Reports from third party vulnerability and security evaluation scanning services
- Vendor security certifications or attestations, such as SOC 2 reports or ISO certifications.
- Records of security testing, such as penetration tests or vulnerability scans, performed on third-party technologies.

EEE-052: Technology Architecture and Design Documentation

- Architecture diagrams and design documents that detail the structure and components of the organization's technology systems, including networks, systems, and applications.
- Records of architecture review board meetings, including decisions on technology design, changes, and rationales for architectural changes.
- Documentation of technology standards, design patterns, and best practices adopted in system design.
- Change history logs and version control records for architectural designs and documents, showing evolution and updates over time.
- Compliance certificates, reports, and assessments verifying that designs and architecture meet relevant industry standards and regulatory requirements.

EEE-099: Technology Delivery and Quality Assurance Documentation

- Project delivery plans that include quality assurance checkpoints and acceptance criteria.
- Quality assurance policies and procedures for technology projects, ensuring deliverables meet specified requirements.
- Records of testing and validation activities, including test plans, results, and defect tracking.
- Post-project reviews or retrospectives focusing on delivery quality and lessons learned.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

GV.RM-08.03: The organization defines, maintains, and uses technical security standards, architectures, processes or practices (including automated tools when practical) to ensure the security of its applications and infrastructure.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #ciso | #compliance | #industry_standards | #policy_management | #review_assessment_and_testing | #security_baselines

Response Guidance:

Provide information on the use of technical security standards, architectures, processes, and practices to ensure the security of applications and infrastructure. Include evidence of technical industry standards used throughout technology and cybersecurity risk management (e.g., SABSA, NIST 800-53, ISO 27001, etc.) Describe and evaluate how these are defined and maintained.

Examples of Effective Evidence:

EEE-023: Third Party Technology Security Assessment and Compliance Documents

- Assessment reports for third party software and technology, including security reviews and compliance checks.
- Documentation of the criteria and standards used for technology assessments.
- Change logs for external software, indicating how updates and patches are managed.
- Reports from third party vulnerability and security evaluation scanning services
- Vendor security certifications or attestations, such as SOC 2 reports or ISO certifications.
- Records of security testing, such as penetration tests or vulnerability scans, performed on third-party technologies.

EEE-036: Vulnerability Scanning and Patch Management Documentation

- Policy, standard, and/or procedure documents covering the identification, assessment, reporting, and remediation of software and device vulnerabilities, including regular patching protocols.
- Schedules and records of patch deployment activities, including system reboots, post-patch testing, dates, systems affected, and patching outcomes.
- Documentation of patching or upgrades to standard system configuration baselines.
- Reports from vulnerability scans or assessments that inform the patch management process.
- Incident reports related to vulnerabilities that were mitigated through patch management.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation and reporting of vulnerability mitigation targets.
- Records of exceptions to, assessments of, and approvals for cases where vulnerability mitigation targets or standards are not met.
- Records demonstrating the integration of patch management and change management practices.
- Approval and review documentation for patching protocols, including impact assessments and authorization records.
- Dashboards or tools used to monitor patch levels and patch application across the target environment.
- Post-implementation reviews and post-change evaluation reports assessing the impact and success of patches and any unintended consequences.
- Audit or review findings related to vulnerability management and patching practices with actions taken in response to findings.

EEE-039: Malware Protection and Incident Detection Documentation

- Anti-malware policies and procedures, including strategies for prevention, detection, and response.
- Logs from anti-malware solutions showing coverage, detection, and remediation of malicious software.
- Exception reports and tracking of malware detection failures and gaps.
- Incident response plans that include specific protocols for handling malware-related incidents.
- Post-incident analysis reports that evaluate the effectiveness of malware protection strategies.

EEE-052: Technology Architecture and Design Documentation

- Architecture diagrams and design documents that detail the structure and components of the organization's technology systems, including networks, systems, and applications.
- Records of architecture review board meetings, including decisions on technology design, changes, and rationales for architectural changes.
- Documentation of technology standards, design patterns, and best practices adopted in system design.
- Change history logs and version control records for architectural designs and documents, showing evolution and updates over time.
- Compliance certificates, reports, and assessments verifying that designs and architecture meet relevant industry standards and regulatory requirements.

EEE-055: Network and System Segmentation Implementation Documentation

- Written policies detailing the approach to network security and system segmentation, including criteria for segmenting resources and strategies for enhancing security.
- Network diagrams showing the segmentation of the network into different zones or segments for security purposes, including firewalls and access control lists.
- Configuration records, change logs, or documentation demonstrating the implementation of segmentation controls.
- Audit reports assessing and evaluating the effectiveness of network and system segmentation in reducing risk, isolating, and protecting critical assets.
- Incident response records showing the role of network segmentation in containing security events.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-056: Operational Technology and IoT Security Documentation

- Security policies and procedures specific to operational technology (OT) and Internet of Things (IoT) devices.
- Inventory lists of OT and IoT devices, including security features and firmware versions.
- Risk assessments for OT and IoT devices, identifying potential vulnerabilities and mitigation strategies.
- Configuration standards for various types of OT and IoT devices (e.g., default password reset).
- Incident response plans that include protocols for addressing security incidents involving OT and IoT devices.
- Documentation of security patches and updates applied to OT and IoT devices, along with testing results.

EEE-057: Remote Access Security and Management Documentation

- Policies governing remote access to the organization's network and systems, including user authentication and authorization procedures and end-user acceptable use policies.
- Records of remote access configurations and settings, ensuring secure connections (e.g., VPN configurations).
- Audit trails or logs of remote access sessions, including user activities and access times.
- Reviews or assessments of remote access security controls, identifying any gaps or improvements needed.
- Training records for employees and contractors on secure remote access practices.

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.
- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

EEE-090: Security and Resilience Design Standards Documents

- Official documents outlining security and resilience architectural and design standards that all technology projects and initiatives must adhere to.
- Checklists and templates used during the design phase of projects to ensure compliance with security and resilience standards.
- Records of design review sessions where security and resilience considerations were evaluated and enforced.
- Case studies or examples of projects that successfully implemented these design standards.
- Audit or review reports assessing adherence to security and resilience design standards across projects.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

GV.RM-08.04: The organization integrates the use of technology architecture in its governance processes to support consistent approaches to security and technology design, integration of third party services, consideration and adoption of new technologies, and investment and procurement decisioning.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #architecture | #mission_and_strategy

Response Guidance:

The organization's technology architecture should be integrated within governance processes to streamline and standardize the risk management activities and support security of the organization's technology. Incorporating the governance with the technology architecture will allow organizations to identify and monitor risks, and develop and implement solutions consistently and within a holistic view. The organization should incorporate governance over the security and technology design, integration of third party services, consideration and adoption of new technologies, and investment and procurement decisioning.

Responses should provide information on how technology architecture is used to ensure security and technology design, third party integration, new technology consideration and adoption, investment and procurement decisioning have consistent organizational governance processes. Describe how the organization consistently manages risk and governs these aspects.

Examples of Effective Evidence:

EEE-052: Technology Architecture and Design Documentation

- Architecture diagrams and design documents that detail the structure and components of the organization's technology systems, including networks, systems, and applications.
- Records of architecture review board meetings, including decisions on technology design, changes, and rationales for architectural changes.
- Documentation of technology standards, design patterns, and best practices adopted in system design.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Change history logs and version control records for architectural designs and documents, showing evolution and updates over time.
- Compliance certificates, reports, and assessments verifying that designs and architecture meet relevant industry standards and regulatory requirements.

EEE-053: Project Governance, Management, and Quality Assurance Documentation

- Project governance frameworks or charters that define roles, responsibilities, and decision-making processes.
- Stakeholder analysis documents and communication plans for engaging with project stakeholders.
- Project management plans that include quality control measures, checkpoints, risk mitigation strategies, and contingency planning.
- Risk assessment templates and completed assessments for technology projects, identifying potential delivery risks.
- Quality assurance policies and procedures for overseeing project deliverables and outcomes.
- Checklists and tools used for quality control during project execution.
- Meeting minutes and action items from project steering committees, governance boards, or risk management discussions within project teams, including actions taken to address identified risks.
- Records of project audits or reviews focused on quality aspects.
- Feedback and satisfaction surveys from stakeholders regarding project outcomes and engagement.
- Reports on project performance, governance effectiveness, and risk management effectiveness, including lessons learned.
- Training documentation for project managers and team members on quality management practices and risk assessment and management techniques.
- Post-project reviews or retrospectives that analyze risk management effectiveness and lessons learned.
- Documentation of project management standards, methodologies, and best practices adopted by the organization

EEE-053: Investment and Procurement Review for Architectural Consistency

- Architecture Review Board (ARB) minutes, procurement reviews, or product analyses
- Presentation decks for purchase recommendations
- Budget submissions, procurement plans, and control gap analyses leading to product purchases
- Vendor due diligence questions addressing consistency with the technology architecture

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GV.RM-08.05: The technology architecture and associated management processes should be comprehensive (e.g., consider the full life cycle of infrastructure, applications, emerging technologies, and relevant data) and designed to achieve security and resilience commensurate with business needs.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #architecture | #mission_and_strategy

Response Guidance:

Describe the organization's governance and management processes used to oversee and implement technology (e.g., infrastructure, applications, emerging technologies, and relevant data). Provide details of how the organization identifies, implements, oversees, manages, and monitors security and resilience requirements within the business and IT environments about how architectures are integrated into these processes.

Examples of Effective Evidence:

EEE-042: Emerging Technology Risk and Opportunity Assessment Documentation

- Strategic reports evaluating the risks and opportunities associated with adopting new or emerging technologies.
- Risk assessment templates and completed assessments for specific technologies under consideration.
- Minutes from meetings or workshops where emerging technologies and their implications were discussed.
- Records of participation in industry events or education related to emerging technologies and risk management.
- Innovation pipeline documents that track the evaluation and adoption process for new technologies.
- Case studies or pilot project reports on the implementation of emerging technologies.

EEE-052: Technology Architecture and Design Documentation

- Architecture diagrams and design documents that detail the structure and components of the organization's technology systems, including networks, systems, and applications.
- Records of architecture review board meetings, including decisions on technology design, changes, and rationales for architectural changes.
- Documentation of technology standards, design patterns, and best practices adopted in system design.
- Change history logs and version control records for architectural designs and documents, showing evolution and updates over time.
- Compliance certificates, reports, and assessments verifying that designs and architecture meet relevant industry standards and regulatory requirements.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

GV.RM-08.06: Technology programs and projects are formally governed and stakeholder engagement is managed to facilitate effective communication, awareness, credible challenge, and decision-making.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #organizational_structure | #staffing_and_resource_management | #training_and_awareness

Response Guidance:

Organizations should establish roles and responsibilities for governance and oversight of the organizations technology programs and projects. The governance should provide credible challenge to the business decisions and operations, facilitate effective communication and reporting structure, and provide awareness of risks, threats, and opportunities. Organizations should organize technology programs and projects to align with stakeholder needs. Program management processes should be in place to regularly communicate to stakeholders on status and progress within expected timeframes, and an agreed upon budget. Organizations should engage with stakeholders to establish priorities and trade-offs between desired functionality and ongoing financial and time investment.

Describe the organization's project management processes consisting of project initiation, planning, execution, and oversight including stakeholder engagement.

Examples of Effective Evidence:

EEE-053: Project Governance, Management, and Quality Assurance Documentation

- Project governance frameworks or charters that define roles, responsibilities, and decision-making processes.
- Stakeholder analysis documents and communication plans for engaging with project stakeholders.
- Project management plans that include quality control measures, checkpoints, risk mitigation strategies, and contingency planning.
- Risk assessment templates and completed assessments for technology projects, identifying potential delivery risks.
- Quality assurance policies and procedures for overseeing project deliverables and outcomes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Checklists and tools used for quality control during project execution.
- Meeting minutes and action items from project steering committees, governance boards, or risk management discussions within project teams, including actions taken to address identified risks.
- Records of project audits or reviews focused on quality aspects.
- Feedback and satisfaction surveys from stakeholders regarding project outcomes and engagement.
- Reports on project performance, governance effectiveness, and risk management effectiveness, including lessons learned.
- Training documentation for project managers and team members on quality management practices and risk assessment and management techniques.
- Post-project reviews or retrospectives that analyze risk management effectiveness and lessons learned.
- Documentation of project management standards, methodologies, and best practices adopted by the organization

EEE-054: Technology Service Performance and Support Monitoring Documentation

- Service level agreements (SLAs) and key performance indicators (KPIs) for technology services and support functions.
- Documentation for service catalogs, service support systems, or other mechanisms for end-users to request services.
- Monitoring dashboards or reports that track service performance against SLAs and KPIs.
- Records of service incidents, including response times, resolution details, and customer feedback.
- Procedures for managing and improving technology service performance.

EEE-099: Technology Delivery and Quality Assurance Documentation

- Project delivery plans that include quality assurance checkpoints and acceptance criteria.
- Quality assurance policies and procedures for technology projects, ensuring deliverables meet specified requirements.
- Records of testing and validation activities, including test plans, results, and defect tracking.
- Post-project reviews or retrospectives focusing on delivery quality and lessons learned.

GV.RM-08.07: Technology projects follow an established project management methodology to manage delivery and delivery risks, produce consistent quality, and achieve business objectives and value.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #mission_and_strategy | #risk_management

Response Guidance:

The organization should follow a standardized project management methodology from project initiation through completion to provide consistency, reliability, and risk management in project delivery and investments. Project management includes but is not limited to system development and

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

acquisition, business process implementation and uplift, resource allocation, system and infrastructure upgrades and maintenance, risk management and assessments, and investments.

Describe the organizations project management methodology. Include details on how the organization identifies, prioritizes, manages, and implements projects. Provide example of project management activities and tracking throughout all stages of the projects lifecycle.

Examples of Effective Evidence:

EEE-003: Strategic Objectives and Planning Documents

- Documentation ot the organization's mission statement.
- Strategic plan outlining the organization's objectives and key results.
- Executive summaries of strategic goals related to IT and cybersecurity.
- Performance reports against strategic objectives.
- Communications from leadership on strategic direction and priorities.

EEE-053: Project Governance, Management, and Quality Assurance Documentation

- Project governance frameworks or charters that define roles, responsibilities, and decision-making processes.
- Stakeholder analysis documents and communication plans for engaging with project stakeholders.
- Project management plans that include quality control measures, checkpoints, risk mitigation strategies, and contingency planning.
- Risk assessment templates and completed assessments for technology projects, identifying potential delivery risks.
- Quality assurance policies and procedures for overseeing project deliverables and outcomes.
- Checklists and tools used for quality control during project execution.
- Meeting minutes and action items from project steering committees, governance boards, or risk management discussions within project teams, including actions taken to address identified risks.
- Records of project audits or reviews focused on quality aspects.
- Feedback and satisfaction surveys from stakeholders regarding project outcomes and engagement.
- Reports on project performance, governance effectiveness, and risk management effectiveness, including lessons learned.
- Training documentation for project managers and team members on quality management practices and risk assessment and management techniques.
- Post-project reviews or retrospectives that analyze risk management effectiveness and lessons learned.
- Documentation of project management standards, methodologies, and best practices adopted by the organization

EEE-099: Technology Delivery and Quality Assurance Documentation

- Project delivery plans that include quality assurance checkpoints and acceptance criteria.
- Quality assurance policies and procedures for technology projects, ensuring deliverables meet specified requirements.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of testing and validation activities, including test plans, results, and defect tracking.
- Post-project reviews or retrospectives focusing on delivery quality and lessons learned.

GOVERN / Risk Management Strategy / Business Continuity & Resilience Risk Management

GV.RM-09.01: The organization has an enterprise-wide resilience strategy and program, including architecture, cyber resilience, business continuity, disaster recovery, and incident response, which support its mission, stakeholder obligations, critical infrastructure role, and risk appetite.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #business_impact_analysis | #critical_infrastructure | #mission_and_strategy | #risk_appetite_/_tolerance | #risk_management

Response Guidance:

The organization should have an enterprise-wide resilience strategy and program because risks in one part of the organization could expose other parts of the organization to harm. Resilience is the ability of an organization to recover from a significant disruption and resume critical operations or operate within a degraded and disrupted operational environment. The enterprise-wide resilience strategy should be incorporated into the overall business strategy and risk management of the organization to ensure consistent, holistic, and integrated response to enterprise operational threats and events. Describe the enterprise-wide cyber resilience (including business continuity, incident response, disaster recovery, and architecture) strategy and program.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.
- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-012: Critical Business Process and Recovery Documentation

- Process and informatioin flow diagrams for critical business operations.
- Business impact analyses that identify and prioritize critical processes.
- Procedures and guidelines for maintaining and operating critical processes.
- Performance metrics and monitoring reports for critical processes.
- Recovery plans for critical business processes in the event of disruption.

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.
- Business continuity plan outlining procedures for maintaining service delivery during disruptions.
- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.
- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.
- Contingency plans detailing alternative service delivery methods.
- Training records for staff on resilience and continuity procedures and their roles during incidents.

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.
- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-016: Recovery Objectives and Strategic Alignment Documentation

- Tools and templates used for formulating recovery strategies that support business objectives.
- A matrix aligning recovery time and point objectives with business priorities.
- Documentation from strategic planning sessions focused on recovery objectives.
- Signed approvals from management endorsing the proposed recovery strategies.
- Periodic review reports assessing the alignment of recovery objectives with business needs.

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-058: Resilience Mechanism Validation and Feedback Documentation

- Plans and procedures for implementing resilience mechanisms across IT systems and business processes.
- Business- and associated system-level requirements for resilience.
- Architecture and design documentation detailing resilience deisgn factors and considerations.
- Schedules and reports from testing and exercises designed to validate the effectiveness of resilience mechanisms.
- Change management documentation related to the enhancement of resilience mechanisms.
- Lessons learned and improvement plans derived from resilience testing activities.
- Stakeholder feedback on the organization's resilience capabilities, gathered through surveys or interviews.

EEE-059: Enterprise and Cyber Resilience Policy Documentation

- Official enterprise resilience strategy documents that outline the organization's approach to achieving and maintaining resilience.
- Cyber resilience policy documents that specify the measures and controls in place to protect against cyber threats.
- Board presentations and approvals related to the resilience strategy and cyber resilience policies.
- Reports from resilience assessments, including gap analyses and recommendations for improvement.

EEE-060: Cross-Sector Incident Response Coordination Documents

- Coordination plans that outline how the organization will work with external entities during an incident response.
- Agreements or MOUs with cross-sector partners and government agencies for collaborative information sharing and/orincident response.
- After-action reports from joint incident response exercises with cross-sector partners.
- Communication protocols for sharing information and coordinating actions during cross-sector incidents.
- Training and exercise records for staff on cross-sector incident response procedures.

EEE-061: Service Recovery and Critical Operations Resumption Documentation

- Procedures and checklists for resuming services and recovering critical operations after an incident.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Prioritization lists that identify critical services and operations for recovery efforts.
- Test results and reports from service resumption drills and recovery exercises.
- Service level agreements (SLAs) with vendors that include provisions for rapid service resumption.
- Documentation of alternative processes and workarounds to be used when primary operations are disrupted.

EEE-078: Resilience Testing and Infrastructure Redundancy Documentation

- Documentation of resilience testing plans and procedures, including objectives, scenarios, and expected outcomes.
- Test reports summarizing the results of resilience testing exercises, highlighting strengths and areas for improvement.
- Infrastructure redundancy designs and implementation records, showing failover capabilities and backup systems.
- Change management records documenting updates or enhancements made to improve infrastructure redundancy.
- Stakeholder feedback on the organization's resilience and redundancy capabilities, gathered after testing or actual events.

EEE-091: Enterprise Resilience Strategy Documentation

- Documentation of the enterprise resilience strategy, outlining objectives, programs, and initiatives designed to enhance organizational resilience.
- Records of resilience program meetings, including strategic decisions, program updates, and progress tracking.
- Training and awareness materials developed to promote resilience across the organization.
- Performance metrics and reports evaluating the effectiveness of resilience programs and initiatives.
- Feedback from internal and external stakeholders on the organization's resilience capabilities and areas for improvement.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EEE-106: Recovery Objectives Critical Infrastructure Documentation

- Documentation of recovery objectives for critical infrastructure and how these align with business continuity goals.
- Critical infrastructure analysis reports that assess the resilience and recovery capabilities of essential systems.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of alignment discussions or decisions between recovery objectives and business needs.
- Audit reports evaluating the alignment of recovery objectives with the criticality of infrastructure components.

EEE-107: Data Recovery and Information Flow Mapping Documentation

- Data recovery strategy documents that outline procedures for restoring lost or corrupted data.
- Information flow maps that illustrate how data moves through the organization, informing recovery planning.
- Test reports from data recovery exercises, demonstrating the ability to restore data in line with recovery strategies.
- Documentation of changes to data recovery strategies based on new business processes or technologies.
- Training records for IT staff on data recovery procedures and information flow considerations.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

EEE-111: Disaster Recovery and Validation Program Documentation

- Disaster Recovery (DR) plans outlining specific recovery steps for Information Technology (IT) systems and data.
- Schedules and results from regular DR testing, ensuring plans are actionable and up-to-date.
- Change management records for DR plans, capturing updates and justifications.
- Records capturing lessons-learned from exercises and the updating of documentation and plans to reflect the improvements.
- Training and certification records for personnel on DR roles and procedures.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Review reports assessing DR plan alignment with overall business recovery objectives and Business Impact Analyses (BIAs).

GV.RM-09.02: The resilience program ensures that the organization can continue operating critical business functions and deliver services to stakeholders, to include critical infrastructure partners, during adverse incidents and cyber attacks (e.g., propagation of malware or extended system outages).

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Subject Tags: #asset_inventory | #asset_management | #business_impact_analysis | #critical_infrastructure | #resilience | #security_logging_monitoring_and_alerting | #technology_availability | #threat_landscape

Response Guidance:

The organization should be capable of operating critical business functions in the face of adverse incidents and cyber attacks. Provide information on how the resilience program ensures that the organization can continue operating critical business functions and deliver services to stakeholders during adverse incidents and cyber attacks (e.g., propagation of malware or extended system outages).

Examples of Effective Evidence:

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.
- Business continuity plan outlining procedures for maintaining service delivery during disruptions.
- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.
- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.
- Contingency plans detailing alternative service delivery methods.
- Training records for staff on resilience and continuity procedures and their roles during incidents.

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-016: Recovery Objectives and Strategic Alignment Documentation

- Tools and templates used for formulating recovery strategies that support business objectives.
- A matrix aligning recovery time and point objectives with business priorities.
- Documentation from strategic planning sessions focused on recovery objectives.
- Signed approvals from management endorsing the proposed recovery strategies.
- Periodic review reports assessing the alignment of recovery objectives with business needs.

EEE-060: Cross-Sector Incident Response Coordination Documents

- Coordination plans that outline how the organization will work with external entities during an incident response.
- Agreements or MOUs with cross-sector partners and government agencies for collaborative information sharing and/orincident response.
- After-action reports from joint incident response exercises with cross-sector partners.
- Communication protocols for sharing information and coordinating actions during cross-sector incidents.
- Training and exercise records for staff on cross-sector incident response procedures.

EEE-061: Service Recovery and Critical Operations Resumption Documentation

- Procedures and checklists for resuming services and recovering critical operations after an incident.
- Prioritization lists that identify critical services and operations for recovery efforts.
- Test results and reports from service resumption drills and recovery exercises.
- Service level agreements (SLAs) with vendors that include provisions for rapid service resumption.
- Documentation of alternative processes and workarounds to be used when primary operations are disrupted.

EEE-075: Malware and Mobile Code Defense Strategy Documents

- Policies and procedures for defending against malware and malicious mobile code, including prevention, detection, and response strategies.
- Configuration records for anti-malware tools and systems, showing protective measures in place.
- Logs and reports from anti-malware solutions, documenting detections and actions taken.
- Post-incident analysis documents that evaluate the response to malware incidents and the effectiveness of defense mechanisms.

EEE-078: Resilience Testing and Infrastructure Redundancy Documentation

- Documentation of resilience testing plans and procedures, including objectives, scenarios, and expected outcomes.
- Test reports summarizing the results of resilience testing exercises, highlighting strengths and areas for improvement.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Infrastructure redundancy designs and implementation records, showing failover capabilities and backup systems.
- Change management records documenting updates or enhancements made to improve infrastructure redundancy.
- Stakeholder feedback on the organization's resilience and redundancy capabilities, gathered after testing or actual events.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

GOVERN / Roles, Responsibilities, and Authorities / Organizational Leadership Responsibility

GV.RR-01.01: The governing authority (e.g., the Board or one of its committees) oversees and holds senior management accountable for implementing the organization's technology and cybersecurity risk management strategies and frameworks.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #risk_management | #risk_oversight | #roles_and_responsibilities

Response Guidance:

The Board (or a board committee) is responsible for the oversight of the organization's technology and cybersecurity risk management program and should ensure compliance with the requirements of the programs by the organization's management, employees, and contractors. The appropriate

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

governing authority may differ by organization (e.g., Senior Management, Executive Management, etc.) but refers to those who should be held accountable for implementing the organization's technology and cybersecurity risk management strategies and frameworks. Accountability requires clear lines of reporting, clear communications, communication of expectations, and the delegation and judicious use of appropriate authority to ensure appropriate compliance with the organization's policies, standards, and procedures.

Include information about relevant board and committee charters (e.g., Board Risk Committee Charter), annual approval of the technology and cybersecurity risk management strategies and frameworks (in addition to the information security program), and terms of reference for any other committees as delegated by the board to review/approve. Describe any related regulatory reporting of the technology and cybersecurity risk management strategies and frameworks. Provide organizational charts to identify responsible/accountable executives.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.
- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Risk management review reports that are presented to the board, including findings and recommendations.
- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.
- Training materials for board members on risk management principles and their oversight responsibilities.

EEE-063: Cybersecurity and Technology Officer Accountability Documents

- Performance goals and objectives set for the Cybersecurity and Technology Officers, including measurable outcomes.
- Documentation of regular reviews or evaluations of the Cybersecurity and Technology Officers' performance.
- Records of decisions and actions taken by these officers, demonstrating their accountability for technology and security outcomes.
- Documentation of any corrective actions or improvements implemented based on performance reviews.
- Evidence of communication by these officers to the board or senior management regarding cybersecurity and technology matters.

EEE-093: Risk Management Strategy and Framework Documentation

- Documentation of the organization's risk management strategy and framework, outlining risk identification, assessment, and mitigation processes.
- Records from risk management framework review sessions, including updates made to adapt to new risks or business changes.
- Risk registers or databases tracking identified risks, assessments, and mitigation actions over time.
- Stakeholder reports summarizing the state of risk management within the organization and strategic recommendations.
- External audit or consultant reviews of the risk management framework, providing independent assessments and suggestions for improvement.

GV.RR-01.02: The governing authority (e.g., the Board or one of its committees) regularly reviews, oversees, and holds senior management accountable for implementing the organization's third-party risk management strategy and program and for managing the organization's ongoing risks associated with the aggregate and specific use of third parties.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #dependency_management | #metrics_and_reporting | #risk_management | #risk_oversight | #third_party_risk_management | #supply_chain_management

Response Guidance:

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

The Board (or a board committee) is responsible for the oversight of the organization's third-party risk management strategy and program and implementing requirements of the program by the organization's management, employees, and contractors. Significant and critical third party engagements should be reviewed and approved by the governing body (e.g., the board or one of its committees). The appropriate governing authority may differ by organization (e.g., Senior Management, Executive Management, etc.) but refers to those who should be held accountable for implementing the organization's third-party risk management strategy and program and for managing the organization's ongoing risks associated with the aggregate and specific use of third parties. The board should review the aggregate use of third parties within the organization's defined risk appetite and risk tolerance. The organization's third-party security policies and procedures should address core governance activities such as oversight and accountability.

Describe how the organization ensures appropriate oversight and compliance with the third-party risk management strategy implementation. Describe how the organization conducts reviews of third-party due diligence to determine if any gaps exist and work towards self-improvement of the program.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-063: Cybersecurity and Technology Officer Accountability Documents

- Performance goals and objectives set for the Cybersecurity and Technology Officers, including measurable outcomes.
- Documentation of regular reviews or evaluations of the Cybersecurity and Technology Officers' performance.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of decisions and actions taken by these officers, demonstrating their accountability for technology and security outcomes.
- Documentation of any corrective actions or improvements implemented based on performance reviews.
- Evidence of communication by these officers to the board or senior management regarding cybersecurity and technology matters.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

GV.RR-01.03: The governing authority (e.g., the Board or one of its committees) regularly reviews, oversees, and holds senior management accountable for implementing the organization's resilience strategy and program and for managing the organization's ongoing resilience risks.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #resilience | #risk_oversight

Response Guidance:

The Board (or a board committee) is responsible for the oversight of the organization's resilience strategy and program and implementing the requirements of the program by the organization's management, employees, and contractors. The appropriate governing authority may differ by organization (e.g., Senior Management, Executive Management, etc.) but refers to those who should be held accountable for implementing the organization's resilience strategy, program and managing ongoing resilience risks. Accountability requires clear lines of reporting, clear communications, communication of expectations, and the delegation and judicious use of appropriate authority to ensure appropriate compliance with the organization's policies, standards, and procedures.

Include information about relevant board and committee charters, annual approval of the resilience strategy and program and terms of reference for any other committees as delegated by the board to review/approve. Describe any related regulatory reporting of the cyber risk management strategy and framework. Provide organizational charts to identify responsible/accountable executives.

Examples of Effective Evidence:

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-059: Enterprise and Cyber Resilience Policy Documentation

- Official enterprise resilience strategy documents that outline the organization's approach to achieving and maintaining resilience.
- Cyber resilience policy documents that specify the measures and controls in place to protect against cyber threats.
- Board presentations and approvals related to the resilience strategy and cyber resilience policies.
- Reports from resilience assessments, including gap analyses and recommendations for improvement.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.
- Risk management review reports that are presented to the board, including findings and recommendations.
- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.
- Training materials for board members on risk management principles and their oversight responsibilities.

EEE-063: Cybersecurity and Technology Officer Accountability Documents

- Performance goals and objectives set for the Cybersecurity and Technology Officers, including measurable outcomes.
- Documentation of regular reviews or evaluations of the Cybersecurity and Technology Officers' performance.
- Records of decisions and actions taken by these officers, demonstrating their accountability for technology and security outcomes.
- Documentation of any corrective actions or improvements implemented based on performance reviews.
- Evidence of communication by these officers to the board or senior management regarding cybersecurity and technology matters.

EEE-091: Enterprise Resilience Strategy Documentation

- Documentation of the enterprise resilience strategy, outlining objectives, programs, and initiatives designed to enhance organizational resilience.
- Records of resilience program meetings, including strategic decisions, program updates, and progress tracking.
- Training and awareness materials developed to promote resilience across the organization.
- Performance metrics and reports evaluating the effectiveness of resilience programs and initiatives.
- Feedback from internal and external stakeholders on the organization's resilience capabilities and areas for improvement.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GV.RR-01.04: The organization has designated a qualified Cybersecurity Officer (e.g., CISO) who is responsible and accountable for developing a cybersecurity strategy, overseeing and implementing its cybersecurity program, and enforcing its cybersecurity policy.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #ciso | #mission_and_strategy | #roles_and_responsibilities | #staffing_and_resource_management

Response Guidance:

Accountability requires clear lines of reporting, clear communication of expectations, and the delegation and judicious use of appropriate authority to ensure compliance with the organization's policies, standards, and procedures. Provide information on the designated and qualified Cybersecurity Officer (e.g., the Chief Information Security Officer (CISO)) and reporting structure, including the Cybersecurity Officer's independence and authority to make risk-based decisions and how the Officer reports to the Board. Additionally, provide information on cybersecurity resources, staff, and tools and how those are assessed against the cybersecurity strategy and any other programs of work to ensure alignment and appropriateness.

Provide information on the budget process being consistent for all businesses and functions across the bank, including the cybersecurity program. For example, describe how software expenses, professional fees, etc. are included in the formal budget processes at both the global and country level. Describe the expenses approval process.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.
- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-031: Cybersecurity and Technology Officer Leadership Documentation

- Job descriptions and role profiles for the Cybersecurity Officer and Technology Officer, outlining responsibilities and qualifications.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Strategic plans and objectives developed by the Cybersecurity Officer and Technology Officer, with documented board or executive approval.
- Records of security initiatives led by these officers, including project plans, status updates, and outcomes.
- Documentation of regular updates or briefings provided to the board and senior management by these officers.
- Evidence of the performance of 360-degree reviews of the Cybersecurity Officer and Technology Officer.
- Performance evaluations or reviews of the Cybersecurity Officer and Technology Officer, assessing their effectiveness and impact.

EEE-032: Technology and Cybersecurity Personnel Roles and Responsibilities Documentation

- Organizational charts and role matrices that clearly define the roles and responsibilities of technology and cybersecurity personnel.
- Training and certification records for staff, demonstrating qualifications and ongoing professional development.
- Policies and procedures that outline the expected contributions of personnel to cybersecurity initiatives.
- Evaluations of skill and resource level requirements against the current personnel complement.
- Incident response team rosters and contact information, indicating roles during security incidents.
- Performance reviews and goal-setting documents for technology and cybersecurity staff.

EEE-063: Cybersecurity and Technology Officer Accountability Documents

- Performance goals and objectives set for the Cybersecurity and Technology Officers, including measurable outcomes.
- Documentation of regular reviews or evaluations of the Cybersecurity and Technology Officers' performance.
- Records of decisions and actions taken by these officers, demonstrating their accountability for technology and security outcomes.
- Documentation of any corrective actions or improvements implemented based on performance reviews.
- Evidence of communication by these officers to the board or senior management regarding cybersecurity and technology matters.

EEE-064: Roles and Responsibilities in Risk Management Documentation

- Organizational charts and job descriptions that clearly define roles and responsibilities related to risk management.
- Documentation of risk management training and awareness programs for personnel across the organization.
- Records of risk-related decisions and actions taken by personnel, showing accountability.
- Performance reviews that include assessments of how individuals manage and mitigate risks within their areas of responsibility.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Incident reports that detail the involvement and effectiveness of personnel in managing and responding to risks.

EEE-103: Security Policy Review and Update Documents

- Security policy review schedules and procedures, including criteria for making updates.
- Change logs or records documenting updates to security policies, including reasons for changes.
- Meeting minutes from stakeholder meetings, capturing input on proposed policy updates.
- Training records for staff on updated security policies and new security requirements.
- Audit or assessment reports that have led to revisions of security policies.

GV.RR-01.05: The organization designates a qualified Technology Officer (e.g., CIO or CTO) who is responsible and accountable for developing technology strategy, overseeing and implementing its technology program, and enforcing its technology policy.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #mission_and_strategy | #policy_management | #risk_oversight | #technology_officer

Response Guidance:

Accountability requires clear lines of reporting, clear communication of expectations, and the delegation and judicious use of appropriate authority to ensure compliance with the organization's policies, standards, and procedures. Provide information on the designated Technology Officer (e.g., CIO or CTO) and reporting structure, including the Technology Officer's independence and authority to make risk-based decisions and how the Officer reports to the Board. Additionally, provide information on technology resources, staff, and tools and how those are assessed against the technology strategy and any other programs of work to ensure alignment and appropriateness.

Provide information on the budget process being consistent for all businesses and functions across the organization, including the technology program. Describe how the designated Technology Officer enforces its technology policy.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.
- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-031: Cybersecurity and Technology Officer Leadership Documentation

- Job descriptions and role profiles for the Cybersecurity Officer and Technology Officer, outlining responsibilities and qualifications.
- Strategic plans and objectives developed by the Cybersecurity Officer and Technology Officer, with documented board or executive approval.
- Records of security initiatives led by these officers, including project plans, status updates, and outcomes.
- Documentation of regular updates or briefings provided to the board and senior management by these officers.
- Evidence of the performance of 360-degree reviews of the Cybersecurity Officer and Technology Officer.
- Performance evaluations or reviews of the Cybersecurity Officer and Technology Officer, assessing their effectiveness and impact.

EEE-032: Technology and Cybersecurity Personnel Roles and Responsibilities Documentation

- Organizational charts and role matrices that clearly define the roles and responsibilities of technology and cybersecurity personnel.
- Training and certification records for staff, demonstrating qualifications and ongoing professional development.
- Policies and procedures that outline the expected contributions of personnel to cybersecurity initiatives.
- Evaluations of skill and resource level requirements against the current personnel complement.
- Incident response team rosters and contact information, indicating roles during security incidents.
- Performance reviews and goal-setting documents for technology and cybersecurity staff.

EEE-063: Cybersecurity and Technology Officer Accountability Documents

- Performance goals and objectives set for the Cybersecurity and Technology Officers, including measurable outcomes.
- Documentation of regular reviews or evaluations of the Cybersecurity and Technology Officers' performance.
- Records of decisions and actions taken by these officers, demonstrating their accountability for technology and security outcomes.
- Documentation of any corrective actions or improvements implemented based on performance reviews.
- Evidence of communication by these officers to the board or senior management regarding cybersecurity and technology matters.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-064: Roles and Responsibilities in Risk Management Documentation

- Organizational charts and job descriptions that clearly define roles and responsibilities related to risk management.
- Documentation of risk management training and awareness programs for personnel across the organization.
- Records of risk-related decisions and actions taken by personnel, showing accountability.
- Performance reviews that include assessments of how individuals manage and mitigate risks within their areas of responsibility.
- Incident reports that detail the involvement and effectiveness of personnel in managing and responding to risks.

GOVERN / Roles, Responsibilities, and Authorities / Risk Management Roles & Responsibilities

GV.RR-02.01: The roles, responsibilities, qualifications, and skill requirements for personnel (employees and third parties) that implement, manage, and oversee the technology, cybersecurity, and resilience programs are defined, aligned, coordinated, and holistically managed.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #roles_and_responsibilities | #staffing_and_resource_management

Response Guidance:

Organizational structure, roles, responsibilities, qualifications, and skill requirements, for levels of authority of the cybersecurity workforce should be clearly established and well-defined especially regarding roles required to handle sensitive data. The roles of personnel (employees and third parties) that implement and directly manage the technology, cybersecurity, and resilience programs are defined, aligned, coordinated, and holistically managed. A shared responsibilities model or similar mechanism should be established to ensure that all appropriate responsibilities are documented, managed, unambiguously assigned, and shared responsibilities are clear between a customer and third party service provider.

Describe the roles and responsibilities throughout the cybersecurity workforce. Describe how management assesses whether the cybersecurity workforce has a reasonable and appropriate level of cybersecurity skills to perform their roles and responsibilities. Provide information related to the roles, responsibilities, and skillsets of personnel who directly manage and oversee the technology, cybersecurity, and resilience programs. Provide information on the role review process and frequency of review. Describe how profiles of specific roles are globally consistent and aligned across the organization.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-032: Technology and Cybersecurity Personnel Roles and Responsibilities Documentation

- Organizational charts and role matrices that clearly define the roles and responsibilities of technology and cybersecurity personnel.
- Training and certification records for staff, demonstrating qualifications and ongoing professional development.
- Policies and procedures that outline the expected contributions of personnel to cybersecurity initiatives.
- Evaluations of skill and resource level requirements against the current personnel complement.
- Incident response team rosters and contact information, indicating roles during security incidents.
- Performance reviews and goal-setting documents for technology and cybersecurity staff.

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.
- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

EEE-095: Security Training and Competency Documentation

- Security awareness and training program documentation, including topics covered, schedules, and target audiences.
- Records of participation and completion for security training sessions, workshops, and e-learning modules.
- Assessments or quizzes measuring employee understanding and retention of security concepts post-training.
- Feedback from employees on the relevance and effectiveness of security training programs.
- Continuous improvement plans for security training, based on feedback, emerging threats, and organizational changes.

GV.RR-02.02: The organization has established and assigned roles and responsibilities for systematic cybersecurity threat identification, monitoring, detection, and event reporting processes, and ensures adequate coverage and organizational alignment for these functions.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #incident_management | #roles_and_responsibilities | #security_logging_monitoring_and_alerting | #threat_management

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Appropriate staff should be responsible for threat identification, monitoring, detection, and reporting suspicious activity. The organization's management should define the responsibility and authority of security personnel and system administrators that perform threat identification, monitoring, detection, and event reporting to ensure there is adequate coverage and organizational alignment. Organizations should establish an organizational unit (e.g., a SOC) that can effectively respond to threats in a timely manner. Organizational coverage and alignment for systematic cybersecurity threat identification, monitoring, detection, and event reporting processes will allow an organization to detect threats early, coordinate responses, effectively act quickly, and improve security posture. Incident response plans should define established escalation protocols and responsibilities for incident management.

Describe the assigned roles and responsibility in place for threat identification, systematic monitoring, detection, and event reporting processes within the organization. Provide program information where applicable.

Examples of Effective Evidence:

EEE-027: Security Event Detection and Categorization Guidelines

- Documentation of the security information and event management (SIEM) system configuration and operational procedures.
- Incident categorization guidelines that define types of incidents and their corresponding response protocols.
- Logs and reports from the SIEM system demonstrating the detection of security events.
- Training materials for security analysts on event detection and incident categorization.
- Audit trails showing the escalation process from event detection to incident declaration.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-068: Threat Monitoring and Detection Program Evaluation Documentation

- Documentation of the monitoring and detection strategies employed to identify potential security threats and vulnerabilities.
- Evaluation reports detailing the effectiveness of monitoring tools and detection mechanisms in identifying and mitigating risks.
- Training records for security personnel on the use of monitoring and detection technologies and techniques.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Change logs demonstrating updates and improvements made to monitoring and detection capabilities.
- Incident case studies showcasing successful detection and response actions facilitated by the monitoring program.

EEE-080: Intrusion Detection and Prevention Systems (IDPS) Documentation

- Policies and procedures governing the operation of intrusion detection and prevention systems (IDPS).
- Configuration and management records for IDPS, detailing rule sets, detection mechanisms, and response actions.
- Logs and alerts generated by IDPS, including analysis of detected intrusions and the effectiveness of prevention measures.
- Audit or review reports assessing the coverage, configuration, and effectiveness of intrusion detection and prevention measures.

GV.RR-02.03: Resilience program roles and responsibilities are assigned to management across the organization to ensure risk assessment, planning, testing, and execution coverage for all critical business functions.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #asset_inventory | #asset_management | #business_impact_analysis | #critical_infrastructure | #resilience | #review_assessment_and_testing | #risk_management | #roles_and_responsibilities | #technology_availability | #threat_management

Response Guidance:

Describe how the organization's resilience program contains clearly defined roles and responsibilities assigned to management and across the organization. Organizational resilience can be achieved by structuring resilience throughout the entire business. The organization may use RACI charts to define leadership, ownership, and accountability of specific roles and responsibilities. Describe how the organization's personnel know their roles and responsibilities to ensure risk assessment, planning, testing, and execution coverage for all critical business functions to ensure timely recovery and resumption of operations.

Examples of Effective Evidence:

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.
- Business continuity plan outlining procedures for maintaining service delivery during disruptions.
- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.
- Contingency plans detailing alternative service delivery methods.
- Training records for staff on resilience and continuity procedures and their roles during incidents.

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.
- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-016: Recovery Objectives and Strategic Alignment Documentation

- Tools and templates used for formulating recovery strategies that support business objectives.
- A matrix aligning recovery time and point objectives with business priorities.
- Documentation from strategic planning sessions focused on recovery objectives.
- Signed approvals from management endorsing the proposed recovery strategies.
- Periodic review reports assessing the alignment of recovery objectives with business needs.

EEE-060: Cross-Sector Incident Response Coordination Documents

- Coordination plans that outline how the organization will work with external entities during an incident response.
- Agreements or MOUs with cross-sector partners and government agencies for collaborative information sharing and/orincident response.
- After-action reports from joint incident response exercises with cross-sector partners.
- Communication protocols for sharing information and coordinating actions during cross-sector incidents.
- Training and exercise records for staff on cross-sector incident response procedures.

GV.RR-02.04: Roles and responsibilities for the Third-Party Risk Management Program and for each third-party engagement are defined and assigned.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #roles_and_responsibilities | #third_party_risk_management | #supply_chain_management

Response Guidance:

All parts of the organization may be involved in third-party risk management (e.g., legal, IT, business management, etc.). As a result, the organization’s management should ensure that roles and responsibilities are clearly defined and assigned for all aspects of the Third-Party Risk Management

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Program and for each third-party engagement including initiation of the relationship, ongoing oversight, and termination. Each third party relationship should have a defined responsible business manager assigned for effective oversight. Provide information on the roles and responsibilities for Third-Party Risk Management Program.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GV.RR-02.05: Personnel (employees and third parties) who fulfill the organization's physical security and cybersecurity objectives understand their roles and responsibilities.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #facilities_management | #physical_security | #roles_and_responsibilities

Response Guidance:

The organization's management should ensure the organization has sufficient expertise to oversee and manage their physical security and cybersecurity objectives. If there are gaps, management should obtain the needed expertise by outsourcing or improving security training for current security staff.

Provide information that supports employees and third parties are informed of their roles and responsibilities (e.g., job descriptions). The performance of their responsibilities is measured on how well they performed, with frequent performance management discussions with direct line management, along with documented annual performance reviews. When outsourced, contractual responsibilities and service level agreements must be clearly defined, and any dependent requirements identified.

Examples of Effective Evidence:

EEE-032: Technology and Cybersecurity Personnel Roles and Responsibilities Documentation

- Organizational charts and role matrices that clearly define the roles and responsibilities of technology and cybersecurity personnel.
- Training and certification records for staff, demonstrating qualifications and ongoing professional development.
- Policies and procedures that outline the expected contributions of personnel to cybersecurity initiatives.
- Evaluations of skill and resource level requirements against the current personnel complement.
- Incident response team rosters and contact information, indicating roles during security incidents.
- Performance reviews and goal-setting documents for technology and cybersecurity staff.

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.
- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-095: Security Training and Competency Documentation

- Security awareness and training program documentation, including topics covered, schedules, and target audiences.
- Records of participation and completion for security training sessions, workshops, and e-learning modules.
- Assessments or quizzes measuring employee understanding and retention of security concepts post-training.
- Feedback from employees on the relevance and effectiveness of security training programs.
- Continuous improvement plans for security training, based on feedback, emerging threats, and organizational changes.

GV.RR-02.06: Roles and responsibilities for the inventory, ownership, and custodianship of applications, data and other technology assets are established and maintained.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #asset_management | #asset_ownership | #critical_infrastructure | #data_classification | #data_lifecycle | #data_protection | #roles_and_responsibilities

Response Guidance:

Describe how the organization establishes and maintains roles and responsibilities for the inventory, and ownership of applications, data, and other technology assets. Describe how the organization inventories assets with their assigned ownership and designates and manages roles and responsibilities for the custodianship. Provide information that supports employees are informed of their roles and responsibilities (e.g., job descriptions, designations of ownership on asset inventories).

Appropriate personnel should be responsible for the inventory, ownership, and custodianship of applications, data, and other technology assets. Describe training for personnel responsible with protecting assets in accordance with its criticality, sensitivity, and usage. Provide information on the role review process and frequency of review.

Examples of Effective Evidence:

EEE-010: IT Asset Management and Business Function Mapping Documentation

- Inventory list of IT assets, including hardware, software, and data.
- Business function catalog that maps key assets to their corresponding business process.
- Asset ownership and stewardship records indicating who is responsible for specific assets.
- Lifecycle management records for assets, showing purchase dates, warranty periods, and disposal information.
- Integration diagrams showing how assets interact within the business's technology ecosystem.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-034: Asset Management and Inventory Oversight Documentation

- Asset management policies that outline the processes and data requirements for tracking, maintaining, and securing organizational assets.
- Inventory lists or databases of assets, including hardware, software, data, and intellectual property, with assigned custodians or owners.
- Change logs or records of asset transfers, disposals, and acquisitions.
- Technical documentation and configuration of automated inventory discovery and management tools.
- Reports from periodic asset audits or reviews, confirming the accuracy of the inventory and compliance with the policy.
- Documentation of asset classification and labeling, indicating the criticality and sensitivity of assets.

GV.RR-02.07: Technology and cybersecurity risk management frameworks provide for segregation of duties between policy development, implementation, and oversight.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #risk_management | #staffing_and_resource_management

Response Guidance:

There should be separate reporting for the information security function from the operational IT environment. Otherwise, the operational IT environment may be placed in the position of self-reporting its own security deficiencies. The organization should assign cybersecurity roles with a clear chain of command that ensures clear reporting up and down the chain of command. This should be reflected in clear, appropriately segmented chains of command.

Describe how policy development, implementation, and oversight responsibilities are covered by different roles within the organization to ensure policies align to the organization's risk tolerance, support the organization's technology and cyber strategy, and consider industry best practices. This may include describing the three lines of defense, relevant policy committee activities, and/or the process for reviewing and approving policies. Provide information on key risk indicator ownership and reporting.

Examples of Effective Evidence:

EEE-064: Roles and Responsibilities in Risk Management Documentation

- Organizational charts and job descriptions that clearly define roles and responsibilities related to risk management.
- Documentation of risk management training and awareness programs for personnel across the organization.
- Records of risk-related decisions and actions taken by personnel, showing accountability.
- Performance reviews that include assessments of how individuals manage and mitigate risks within their areas of responsibility.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Incident reports that detail the involvement and effectiveness of personnel in managing and responding to risks.

EEE-066: Segregation of Duties in Risk Management Documentation

- Policies and procedures that establish segregation of duties within risk management activities to prevent conflicts of interest and fraud.
- Flowcharts or diagrams that illustrate the separation of roles and responsibilities in risk-related processes.
- Internal control reports that verify the effectiveness of segregation of duties in mitigating risks.
- Records of changes to duties or responsibilities to maintain proper segregation as the organization evolves.

GOVERN / Roles, Responsibilities, and Authorities / Resource Adequacy

GV.RR-03.01: The organization's budgeting and resourcing processes identify, prioritize, and address resource needs to manage identified technology and cybersecurity risks (e.g., skill shortages, headcount, new tools, incident-related expenses, and unsupported systems).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #enterprise_risk_management | #staffing_and_resource_management

Response Guidance:

Resources, including funding and technical/managerial talent, contribute to the effectiveness of the technology and cyber risk management program. The program should be staffed by enough personnel with skills aligned to the organization's technical and managerial needs and commensurate with its size, complexity, and risk profile. Management should have a methodology in place to measure and document technology and cybersecurity risks to determine resources required for mitigating gaps. Unsupported systems and legacy systems should be considered throughout budgeting and resourcing processes to mitigate resourcing gaps and risks. The Board should review and approve the cyber risk mitigation plans and the allocation of the required resources.

Response should include how resourcing is evaluated within the technology and cyber risk management framework and support structures. Provide information on the resourcing review scope and cycle along with roles and responsibilities of those involved in the resourcing assessment and approvals. Provide information on Board, committee, and/or senior management review and approval of prioritization and resource allocations related to technology and cybersecurity improvement programs.

Examples of Effective Evidence:

EEE-032: Technology and Cybersecurity Personnel Roles and Responsibilities Documentation

- Organizational charts and role matrices that clearly define the roles and responsibilities of technology and cybersecurity personnel.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Training and certification records for staff, demonstrating qualifications and ongoing professional development.
- Policies and procedures that outline the expected contributions of personnel to cybersecurity initiatives.
- Evaluations of skill and resource level requirements against the current personnel complement.
- Incident response team rosters and contact information, indicating roles during security incidents.
- Performance reviews and goal-setting documents for technology and cybersecurity staff.

EEE-067: Resource Planning and Allocation for Risk Management Documentation

- Strategic plans that include resource allocation for risk management functions, such as staffing, technology, and training.
- Budget documents that detail funding dedicated to risk management activities.
- Capacity and resiliency planning reports that assess the resources needed to effectively manage risks.
- Documentation of resource adjustments made in response to changes in the risk landscape.
- Records of resource utilization and efficiency in risk management, including return on investment analyses.

GV.RR-03.02: The organization regularly assesses its skill and resource level requirements against its current personnel complement to determine gaps in resource need.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #human_resources | #staffing_and_resource_management | #training_and_awareness

Response Guidance:

Describe how the organization regularly assesses its skill and resource level requirements against its current personnel to determine gaps in resource need. Describe how the organization allocates funding and budgets for resources to support robust technology and cybersecurity programs.

Describe how resources are assessed against the technology and cybersecurity strategy and programs to work to ensure alignment, appropriateness, and gaps in resource need. Describe the funding and budget processes, including how the budget is created and approved, and how the organization makes changes to the budget.

Examples of Effective Evidence:

EEE-032: Technology and Cybersecurity Personnel Roles and Responsibilities Documentation

- Organizational charts and role matrices that clearly define the roles and responsibilities of technology and cybersecurity personnel.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Training and certification records for staff, demonstrating qualifications and ongoing professional development.
- Policies and procedures that outline the expected contributions of personnel to cybersecurity initiatives.
- Evaluations of skill and resource level requirements against the current personnel complement.
- Incident response team rosters and contact information, indicating roles during security incidents.
- Performance reviews and goal-setting documents for technology and cybersecurity staff.

EEE-064: Roles and Responsibilities in Risk Management Documentation

- Organizational charts and job descriptions that clearly define roles and responsibilities related to risk management.
- Documentation of risk management training and awareness programs for personnel across the organization.
- Records of risk-related decisions and actions taken by personnel, showing accountability.
- Performance reviews that include assessments of how individuals manage and mitigate risks within their areas of responsibility.
- Incident reports that detail the involvement and effectiveness of personnel in managing and responding to risks.

EEE-067: Resource Planning and Allocation for Risk Management Documentation

- Strategic plans that include resource allocation for risk management functions, such as staffing, technology, and training.
- Budget documents that detail funding dedicated to risk management activities.
- Capacity and resiliency planning reports that assess the resources needed to effectively manage risks.
- Documentation of resource adjustments made in response to changes in the risk landscape.
- Records of resource utilization and efficiency in risk management, including return on investment analyses.

EEE-095: Security Training and Competency Documentation

- Security awareness and training program documentation, including topics covered, schedules, and target audiences.
- Records of participation and completion for security training sessions, workshops, and e-learning modules.
- Assessments or quizzes measuring employee understanding and retention of security concepts post-training.
- Feedback from employees on the relevance and effectiveness of security training programs.
- Continuous improvement plans for security training, based on feedback, emerging threats, and organizational changes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GV.RR-03.03: The organization provides adequate resources, appropriate authority, and access to the governing authority for the designated Cybersecurity Officer (e.g., CISO).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #ciso | #staffing_and_resource_management

Response Guidance:

The organization's management should ensure the organization has sufficient expertise to oversee and manage their cybersecurity operations. Funding, along with technical and managerial talent, contributes to the effectiveness of the cybersecurity program. Provide information on how the designated Cybersecurity Officer (e.g., CISO) has adequate resources, appropriate authority, and access. Provide information on how the organization Describe how the organization institutes specific programs of work to increase cybersecurity maturity. Provide information on how additional cybersecurity resources, staff, and tools are assessed against the cybersecurity strategy and programs of work to ensure alignment and appropriateness. Describe the budget process for cybersecurity, including how the budget is created and approved, and how the organization makes changes to the budget.

Describe the use of external security review vendors (if applicable) combined with annual audit and regulatory reviews that assist with identification of cybersecurity tools and expertise that may be needed to fill any needs.

Describe what specific training is in place to assist in evolving current staff to current emerging threat landscape.

Examples of Effective Evidence:

EEE-031: Cybersecurity and Technology Officer Leadership Documentation

- Job descriptions and role profiles for the Cybersecurity Officer and Technology Officer, outlining responsibilities and qualifications.
- Strategic plans and objectives developed by the Cybersecurity Officer and Technology Officer, with documented board or executive approval.
- Records of security initiatives led by these officers, including project plans, status updates, and outcomes.
- Documentation of regular updates or briefings provided to the board and senior management by these officers.
- Evidence of the performance of 360-degree reviews of the Cybersecurity Officer and Technology Officer.
- Performance evaluations or reviews of the Cybersecurity Officer and Technology Officer, assessing their effectiveness and impact.

EEE-032: Technology and Cybersecurity Personnel Roles and Responsibilities Documentation

- Organizational charts and role matrices that clearly define the roles and responsibilities of technology and cybersecurity personnel.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Training and certification records for staff, demonstrating qualifications and ongoing professional development.
- Policies and procedures that outline the expected contributions of personnel to cybersecurity initiatives.
- Evaluations of skill and resource level requirements against the current personnel complement.
- Incident response team rosters and contact information, indicating roles during security incidents.
- Performance reviews and goal-setting documents for technology and cybersecurity staff.

EEE-064: Roles and Responsibilities in Risk Management Documentation

- Organizational charts and job descriptions that clearly define roles and responsibilities related to risk management.
- Documentation of risk management training and awareness programs for personnel across the organization.
- Records of risk-related decisions and actions taken by personnel, showing accountability.
- Performance reviews that include assessments of how individuals manage and mitigate risks within their areas of responsibility.
- Incident reports that detail the involvement and effectiveness of personnel in managing and responding to risks.

EEE-067: Resource Planning and Allocation for Risk Management Documentation

- Strategic plans that include resource allocation for risk management functions, such as staffing, technology, and training.
- Budget documents that detail funding dedicated to risk management activities.
- Capacity and resiliency planning reports that assess the resources needed to effectively manage risks.
- Documentation of resource adjustments made in response to changes in the risk landscape.
- Records of resource utilization and efficiency in risk management, including return on investment analyses.

GOVERN / Roles, Responsibilities, and Authorities / Human Resource Practices

GV.RR-04.01: The organization conducts (or causes the conduct of) background/screening checks on all personnel (employees and third party) upon hire/retention, at regular intervals throughout employment, and upon a change in role commensurate with their access to critical data and systems.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #background_checks | #business_impact_analysis | #critical_infrastructure | #fraud | #human_resources | #roles_and_responsibilities | #vendor_management

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

The organization should conduct background verifications for prospective employees and third parties with access to confidential or sensitive data, systems, or facilities. Furthermore, background checks should be conducted at regular intervals and upon change to the employee or third party's role. The organization may conduct background checks on third-party personnel directly or may employ contract clauses to ensure that background checks are performed by the third-party to approved standards. Background checks should be conducted in accordance with local laws, rules, and regulations.

Describe how the organization conducts background/screening checks on all employees. If legal restrictions limit the scope of verification, then procedures should be defined consistent with the sensitivity of the data and processes being accessed, business requirements, or other legal considerations. Provide information on the governance and processes utilized for conducting background checks.

Examples of Effective Evidence:

EEE-018: Supplier Evaluation, Onboarding, and Due Diligence Documentation

- Checklists and criteria used for evaluating potential suppliers, including security and resilience factors.
- Due diligence reports for key suppliers, including assessments of their financial stability and operational resilience.
- Agreements that include clauses related to ongoing monitoring and evaluation of supplier performance.
- Records of supplier selection meetings, including rationale for decisions and any identified risks.
- Supplier onboarding process documentation, highlighting security and resilience requirements.

EEE-108: Background and Screening Checks Documents

- Policies and procedures for conducting background checks and screening of employees, contractors, and third parties.
- Records of completed background checks and screenings, including dates and outcomes.
- Compliance reports verifying that background and screening practices meet legal and regulatory requirements.
- Audit trails showing the integration of background check results into hiring or contracting decisions.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GV.RR-04.02: The organization establishes processes and controls to mitigate cyber risks related to employment termination, as permitted by law, to include the return or disposition of all organizational assets.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #access_management | #asset_management | #data_loss_prevention | #identity_and_access_management | #insider_threat | #physical_access | #risk_management | #security_logging_monitoring_and_alerting

Response Guidance:

Access management policies and procedures should establish a process for terminating users. If an organization terminates an individual's employment, there should be measures in place that require that user's access to any asset or system be removed immediately, including proprietary information (e.g., customer lists, etc.). The organization may put additional monitoring in place when an employee provides notice of termination (e.g., social media monitoring, data loss prevention, other security monitoring tools).

Describe how the organization has established processes and controls to mitigate cyber risks related to employment termination, in consideration of legal restrictions, if any. Provide information on the termination process and related controls to include the return or disposition of all organizational assets.

Examples of Effective Evidence:

EEE-026: Third-Party Termination and Decommissioning Documentation

- Termination procedures and checklists that outline the steps for ending a relationship with a third party.
- Documentation of data retrieval or transfer processes upon termination of a third-party contract.
- Records of final account settlements and confirmations of service discontinuation.
- Technical closure reports that confirm the secure decommissioning of third-party services and systems.
- Exit interview records or final performance reviews with the third party, capturing lessons learned and final assessments.

EEE-034: Asset Management and Inventory Oversight Documentation

- Asset management policies that outline the processes and data requirements for tracking, maintaining, and securing organizational assets.
- Inventory lists or databases of assets, including hardware, software, data, and intellectual property, with assigned custodians or owners.
- Change logs or records of asset transfers, disposals, and acquisitions.
- Technical documentation and configuration of automated inventory discovery and management tools.
- Reports from periodic asset audits or reviews, confirming the accuracy of the inventory and compliance with the policy.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of asset classification and labeling, indicating the criticality and sensitivity of assets.

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

GV.RR-04.03: The organization integrates insider threat considerations into its human resource, risk management, and control programs to address the potential for malicious or unintentional harm by trusted employees or third parties.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #background_checks | #fraud | #insider_threat | #physical_access | #risk_management | #security_logging_monitoring_and_alerting

Response Guidance:

Describe how insider threat considerations are integrated into human resource practices (e.g., personnel screening), risk management (e.g., risk mitigation, operational resilience), and control programs (e.g., access controls, continuous monitoring). Risk management frameworks, plans, standards, and procedures should be inclusive of insider threat considerations and not limited to external actors. Organizations can enforce separation of duties and least privilege to limit malicious or unintentional harm by trusted employees or third parties.

Provide information on how the organization conducts background/screening checks upon hire and at regular intervals throughout employment, and upon a change in role. Training programs should be in place for processes to recognize and report suspicious behavior. Describe the framework for integrating human resources and legal considerations to ensure that employee rights are protected including in the conduct of investigations of suspected misbehavior.

Describe how control programs integrate insider threat considerations. Describe how access, detection, monitoring, and auditing controls are utilized to detect anomalous activities and insider threats.

Examples of Effective Evidence:

EEE-006: Cybersecurity, Culture, and Training Record Documents

- Employee cybersecurity awareness survey results.
- Training attendance logs for cybersecurity and IT policy courses.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Assessments of organizational culture regarding security practices.
- Feedback and improvement reports following culture assessments.
- Records of cultural change initiatives related to cybersecurity.

EEE-033: Training Programs Documents and Physical and Cybersecurity Documentation

- Documented physical and cybersecurity objectives aligned with the organization's overall security strategy.
- Training curricula and schedules for physical and cybersecurity awareness and skill-building programs.
- Attendance records and completion certificates for security training sessions.
- Evaluations and feedback from participants on the effectiveness of the training programs.
- Security exercise and drill reports, demonstrating the application of training in simulated scenarios.

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.
- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

EEE-043: Cybersecurity Training, Awareness, and Expertise Access Documentation

- Agendas and materials from cybersecurity awareness events and training sessions.
- Records of accessing/retaining cybersecurity expertise and resources, including external consultants or internal experts.
- Partnerships with educational institutions or professional organizations to enhance cybersecurity knowledge.
- Records of employee participation in external cybersecurity conferences, workshops, or courses.
- Feedback from employees on the accessibility and usefulness of cybersecurity training and expertise.

EEE-108: Background and Screening Checks Documents

- Policies and procedures for conducting background checks and screening of employees, contractors, and third parties.
- Records of completed background checks and screenings, including dates and outcomes.
- Compliance reports verifying that background and screening practices meet legal and regulatory requirements.
- Audit trails showing the integration of background check results into hiring or contracting decisions.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GOVERN / Policies, Processes, and Procedures / Establishment of Policies & Procedures

GV.PO-01.01: Technology and cybersecurity policies are documented, maintained and approved by the governing authority (e.g., the Board or one of its committees) or a designated executive.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #policy_management

Response Guidance:

The organization should have technology and cybersecurity policies, standards and procedures that align with risk and complexity and are approved by the governing authority (e.g., the Board or one of its committees) or a designated qualified executive. Generally, the technology and cybersecurity policies should include all operations and business processes supported by technology and define clear management accountability, to include responsibilities of staff that contribute to the development of the policies. The Board or one of its committees is responsible for overseeing the organization's technology and cybersecurity program, including reviewing and approving technology and cybersecurity policies.

Provide information regarding the organizational structure for the management and operation of technology and cybersecurity enacted through policies and procedures, as well as governance forums for the management of controls. Describe how the Information Security Program is approved by the appropriate governing authority (e.g., Board Risk Committee) or designated executive. Describe how the Information Security Program is updated on a regular basis. Describe how technology and cybersecurity standards are defined by the cyber team and how the policies are regularly updated and reviewed by subject matter experts.

Examples of Effective Evidence:

EEE-002: Board Governance and IT Oversight Documentation

- Board of Directors' charter and governance guidelines.
- Copies of presentations, reports, and minutes from board meetings and committees related to IT and cybersecurity.
- Records of decisions and actions taken regarding IT governance.
- Policy documents on roles and responsibilities of governance bodies.
- Compliance reports related to governance policies and practices.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.
- Risk management review reports that are presented to the board, including findings and recommendations.
- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Training materials for board members on risk management principles and their oversight responsibilities.

EEE-103: Security Policy Review and Update Documents

- Security policy review schedules and procedures, including criteria for making updates.
- Change logs or records documenting updates to security policies, including reasons for changes.
- Meeting minutes from stakeholder meetings, capturing input on proposed policy updates.
- Training records for staff on updated security policies and new security requirements.
- Audit or assessment reports that have led to revisions of security policies.

GV.PO-01.02: The accountable governing body, and applicable cybersecurity program and policies, for any given organizational unit, affiliate, or merged entity are clearly established, applied, and communicated.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #board_or_committee_oversight | #policy_management

Response Guidance:

An affiliate of a financial institution may include a company that controls the institution (i.e., holding company), a subsidiary of the institution, or any company with a relationship constituting an affiliate under applicable regulations. The organization may adopt security program(s) of its affiliate(s) if such program provides a level of control and assurance appropriate to the risk and complexity of the organization. Furthermore, the accountable governing body and cybersecurity program, policies, and standards for an any given organizational unit, merged entity, or affiliate must be defined, applied, and communicated to all staff.

If applicable, describe how the organization adopts the security program of affiliates and provide evidence that the program provides an appropriate level of control and assurance.

Examples of Effective Evidence:

EEE-002: Board Governance and IT Oversight Documentation

- Board of Directors' charter and governance guidelines.
- Copies of presentations, reports, and minutes from board meetings and committees related to IT and cybersecurity.
- Records of decisions and actions taken regarding IT governance.
- Policy documents on roles and responsibilities of governance bodies.
- Compliance reports related to governance policies and practices.

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-031: Cybersecurity and Technology Officer Leadership Documentation

- Job descriptions and role profiles for the Cybersecurity Officer and Technology Officer, outlining responsibilities and qualifications.
- Strategic plans and objectives developed by the Cybersecurity Officer and Technology Officer, with documented board or executive approval.
- Records of security initiatives led by these officers, including project plans, status updates, and outcomes.
- Documentation of regular updates or briefings provided to the board and senior management by these officers.
- Evidence of the performance of 360-degree reviews of the Cybersecurity Officer and Technology Officer.
- Performance evaluations or reviews of the Cybersecurity Officer and Technology Officer, assessing their effectiveness and impact.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.
- Risk management review reports that are presented to the board, including findings and recommendations.
- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.
- Training materials for board members on risk management principles and their oversight responsibilities.

GV.PO-01.03: The organization's incentive programs are consistent with cyber risk management objectives, and technology and cybersecurity policies integrate with an employee accountability policy to ensure that all personnel are held accountable for complying with policies.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #policy_management | #review_assessment_and_testing | #staffing_and_resource_management

Response Guidance:

Management should implement incentive programs consistent with cyber risk management objectives to ensure employees know and understand their technology and cybersecurity responsibilities. Employees should provide explicit attestations indicating that they have read, understand, and agree to abide by the rules that describe their responsibilities and expected behavior

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

regarding their technology and cybersecurity roles and responsibilities. For instance, employees may be required to review and signoff on technology and cybersecurity policies annually. Policies should also provide for disciplinary action if the employee fails to follow them.

Provide information on assigned training (e.g., code of conduct including consequence management and mandatory training policy). In addition, provide any information and technology and cybersecurity policies that integrate with an employee accountability policy that may require assigned information and cybersecurity risk situational awareness training.

Examples of Effective Evidence:

EEE-006: Cybersecurity, Culture, and Training Record Documents

- Employee cybersecurity awareness survey results.
- Training attendance logs for cybersecurity and IT policy courses.
- Assessments of organizational culture regarding security practices.
- Feedback and improvement reports following culture assessments.
- Records of cultural change initiatives related to cybersecurity.

EEE-033: Training Programs Documents and Physical and Cybersecurity Documentation

- Documented physical and cybersecurity objectives aligned with the organization's overall security strategy.
- Training curricula and schedules for physical and cybersecurity awareness and skill-building programs.
- Attendance records and completion certificates for security training sessions.
- Evaluations and feedback from participants on the effectiveness of the training programs.
- Security exercise and drill reports, demonstrating the application of training in simulated scenarios.

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.
- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

GV.PO-01.04: All personnel (employees and third party) consent to policies addressing acceptable technology use, social media use, personal device use (e.g., BYOD), confidentiality, and/or other security-related policies and agreements as warranted by their position.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #end_user_security | #policy_management | #review_assessment_and_testing | #social_media

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Provide information on established policies, procedures, and agreements for defining and permitting use of acceptable technology, social media, and personal devices for all personnel (employees and third party). Describe how the acceptable use policies, procedures, and agreements permit access to the organization's information systems and networks. Inappropriate use exposes the organization to potential risks (e.g., unauthorized access, compromise of network systems). Policies for personal device (e.g., BYOD) should be established to separate work and personal data that is aligned with other security-related policies, risk assessments, and other agreements as warranted by their position to help protect an organization's information that is on a personally owned device.

Describe how the organization implements mechanisms to restrict access to websites or services that do not serve legitimate business needs or purposes. Provide information on approval and authorization processes for all personnel to access the organization's applications and network through personnel devices. Describe the process of all personnel reviewing and accepting acceptable use policies.

Examples of Effective Evidence:

EEE-008: Customer Data Privacy and Data Protection Documentation

- Published privacy policy detailing how customer data is handled and protected.
- Consent forms and records of customer approvals for data processing.
- Data Protection Impact Assessments (DPIAs) for new projects involving personal data.
- Records of privacy policy reviews and updates.
- Documentation of customer notifications in the event of a data breach.

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.
- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

GV.PO-01.05: Technology and cybersecurity processes, procedures, and controls are established in alignment with cybersecurity policy.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #policy_management

Response Guidance:

Provide information describing how an organization's technology and cybersecurity processes, procedures, and controls align with an organization's cybersecurity policy. Explain how the information and technology and cybersecurity strategy integrates technology, policies, procedures,

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

controls, and training to mitigate risk. Describe how technology and cybersecurity standards are defined, who reviews these standards, and what processes exist for updating standards. Show the taxonomy and relationship of policies, standards, controls, and processes/procedures within the organization.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.
- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-094: Technology and Cybersecurity Risk Appetite Documents

- Official statements or documents defining the organization's risk appetite specifically related to technology and cybersecurity.
- Board or executive committee meeting minutes discussing and approving the risk appetite statement.
- Guidelines for aligning IT and cybersecurity initiatives with the defined risk appetite.
- Reviews or assessments of projects and initiatives to ensure they are within the organization's technology and cybersecurity risk appetite.

EEE-103: Security Policy Review and Update Documents

- Security policy review schedules and procedures, including criteria for making updates.
- Change logs or records documenting updates to security policies, including reasons for changes.
- Meeting minutes from stakeholder meetings, capturing input on proposed policy updates.
- Training records for staff on updated security policies and new security requirements.
- Audit or assessment reports that have led to revisions of security policies.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GV.PO-01.06: Physical and environmental security policies are implemented and managed.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #facilities_management | #physical_security | #policy_management

Response Guidance:

Physical security controls vary according to the assets at risk (e.g., data, infrastructure, systems). For example, data centers commonly house a financial institution's data repositories and most critical systems. In this case, management should consider physical controls that address all internal and external threats (e.g., unauthorized access, theft, damage) and environmental threats inherent to physical locations. Physical controls may involve devices that detect adverse events and help prevent theft and safeguard the equipment, like surveillance. The devices should provide continuous coverage, send alarms when responses are necessary, and support investigations.

Describe the implementation and management of the physical and environmental security policies. Describe where management of the physical and environmental security responsibility resides within the organization.

Describe how the organization manages compliance with physical and environmental security policies, such as through security logs or other protective security measures.

Examples of Effective Evidence:

EEE-033: Training Programs Documents and Physical and Cybersecurity Documentation

- Documented physical and cybersecurity objectives aligned with the organization's overall security strategy.
- Training curricula and schedules for physical and cybersecurity awareness and skill-building programs.
- Attendance records and completion certificates for security training sessions.
- Evaluations and feedback from participants on the effectiveness of the training programs.
- Security exercise and drill reports, demonstrating the application of training in simulated scenarios.

EEE-077: Physical and Environmental Security Documents

- Documentation of environmental controls (e.g., fire suppression, climate control) and physical security measures (e.g., access controls, surveillance systems).
- Maintenance and inspection records for environmental and physical security equipment.
- Incident logs related to environmental hazards or physical security breaches, including responses and outcomes.
- Security audit reports evaluating the adequacy of environmental and physical security controls.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GV.PO-01.07: The organization maintains documented business continuity and resilience program policies and procedures approved by the governing authority (e.g., the Board or one of its committees).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #policy_management | #resilience | #risk_oversight

Response Guidance:

Provide information supporting the organization's business continuity and resilience program policies and procedures have been reviewed and approved by the governing authority (e.g., the Board or one of its committees). Business continuity and resilience program, policies, and procedures should be reviewed and approved regularly to ensure an organization can maintain, resume, and recover critical business functions and processes during and following an incident.

Examples of Effective Evidence:

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.
- Business continuity plan outlining procedures for maintaining service delivery during disruptions.
- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.
- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.
- Contingency plans detailing alternative service delivery methods.
- Training records for staff on resilience and continuity procedures and their roles during incidents.

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.
- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-059: Enterprise and Cyber Resilience Policy Documentation

- Official enterprise resilience strategy documents that outline the organization's approach to achieving and maintaining resilience.
- Cyber resilience policy documents that specify the measures and controls in place to protect against cyber threats.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Board presentations and approvals related to the resilience strategy and cyber resilience policies.
- Reports from resilience assessments, including gap analyses and recommendations for improvement.

EEE-069: Crisis Response and Business Continuity Management Documentation

- Crisis response plans that detail specific actions, communication protocols, templates, and roles during various crisis scenarios.
- Exercise and drill records, including scenarios, outcomes, and lessons learned, to validate crisis response capabilities.
- After-action reports from actual crisis events, analyzing the response effectiveness and areas for improvement.
- Stakeholder feedback on the organization's response during crisis situations, used to refine continuity and crisis response plans.

EEE-086: Recovery Strategy and Resilience Plan Documentation

- Documentation of the organization's recovery strategies, including plans for restoring critical services and operations after an incident.
- Change logs or records showing updates to recovery strategies and resilience plans based on lessons learned from exercises or actual incidents.
- Stakeholder feedback and review summaries that have led to updates in recovery strategies or resilience plans.
- Training session records for staff on updated recovery procedures and resilience measures.
- Audit reports or assessments that have identified areas for improvement in recovery strategies, leading to plan updates.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

GV.PO-01.08: The organization maintains documented third-party risk management program policies and procedures approved by the governing authority (e.g., the Board or one of its committees).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #policy_management | #risk_oversight | #third_party_risk_management | #supply_chain_management

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Provide information supporting the organization's third-party risk management policies and procedures have been reviewed and approved by the governing authority (e.g., the Board or one of its committees) and updated on a regularly basis. For example, policies may include a page indicating when it was last updated and who reviewed it. Describe how third-party risk management policies and procedures are regularly updates and reviewed by the governing authority.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.
- Risk management review reports that are presented to the board, including findings and recommendations.
- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.
- Training materials for board members on risk management principles and their oversight responsibilities.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GOVERN / Policies, Processes, and Procedures / Policy & Procedure Review & Update

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

GV.PO-02.01: The cybersecurity policy is regularly reviewed, revised, and communicated under the leadership of a designated Cybersecurity Officer (e.g., CISO) to address changes in the risk profile and risk appetite, the evolving threat environment, and new technologies, products, services, and interdependencies.

Subject Tags: #policy_management | #risk_appetite_/_tolerance | #risk_management

Response Guidance:

The organization, under the leadership of the designated Cybersecurity Officer (e.g., CISO), should have a formal process that reviews and updates all cybersecurity-related policies across business lines periodically.

Describe responsibility, process, and frequency for reviewing/revising policies. As new or enhanced cybersecurity regulations are published (trigger event(s)), new technologies, products, services become available or new cyber risks and threats are identified, show how policies are reviewed to ensure alignment or identify gaps (e.g., how trigger event(s) are consumed by the organization and updated in policies). Describe how the policy team communicates policy changes. Describe if annual training includes changes to policies.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.
- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-002: Board Governance and IT Oversight Documentation

- Board of Directors' charter and governance guidelines.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Copies of presentations, reports, and minutes from board meetings and committees related to IT and cybersecurity.
- Records of decisions and actions taken regarding IT governance.
- Policy documents on roles and responsibilities of governance bodies.
- Compliance reports related to governance policies and practices.

EEE-031: Cybersecurity and Technology Officer Leadership Documentation

- Job descriptions and role profiles for the Cybersecurity Officer and Technology Officer, outlining responsibilities and qualifications.
- Strategic plans and objectives developed by the Cybersecurity Officer and Technology Officer, with documented board or executive approval.
- Records of security initiatives led by these officers, including project plans, status updates, and outcomes.
- Documentation of regular updates or briefings provided to the board and senior management by these officers.
- Evidence of the performance of 360-degree reviews of the Cybersecurity Officer and Technology Officer.
- Performance evaluations or reviews of the Cybersecurity Officer and Technology Officer, assessing their effectiveness and impact.

EEE-103: Security Policy Review and Update Documents

- Security policy review schedules and procedures, including criteria for making updates.
- Change logs or records documenting updates to security policies, including reasons for changes.
- Meeting minutes from stakeholder meetings, capturing input on proposed policy updates.
- Training records for staff on updated security policies and new security requirements.
- Audit or assessment reports that have led to revisions of security policies.

GOVERN / Oversight / Risk Management Strategy Outcomes Review

GV.OV-01.01: The governing authority (e.g., the Board or one of its committees) regularly reviews and evaluates the organization's ability to manage its technology, cybersecurity, third-party, and resilience risks.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #risk_management | #risk_oversight | #roles_and_responsibilities

Response Guidance:

The organization should have a process for evaluating changes to the organization's technology, cybersecurity, third-party, and resilience risks. The process should ensure that management updates the cyber risk management strategy, as needed, to effectively address emerging threats, vulnerabilities, and changes in risk internal and external to the organization.

Provide information that demonstrates the appropriate governing authority reviews (scope, frequency, etc.) and evaluates the effectiveness with which the organization can manage its technology,

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

cybersecurity, third-party, and resilience risks. Include examples of information provided to the governing authority.

Examples of Effective Evidence:

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.
- Risk management review reports that are presented to the board, including findings and recommendations.
- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.
- Training materials for board members on risk management principles and their oversight responsibilities.

GV.OV-01.02: The designated Cybersecurity Officer (e.g., CISO) periodically reports to the appropriate governing authority (e.g., the Board or one of its committees) or equivalent governing body on the status of cybersecurity within the organization.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #ciso | #metrics_and_reporting

Response Guidance:

The organization should develop, present, and discuss cyber risk reporting, enabling management to measure, monitor, and control cyber risk to the fullest extent possible. The designated Cybersecurity Officer (e.g., CISO) should provide a report on the status and effectiveness of the cybersecurity program to the Board of Directors regularly.

Describe how the CISO presents on the cybersecurity control environment for the management of the organization's cybersecurity risk posture through the management and operation of security controls. Provide information on how the designated Cybersecurity Officer reports to the Board Risk Committee. Additionally, provide information regarding presentations to the Board of Directors by the designated Cybersecurity Officer, in annual or quarterly meetings, including updates on topics such

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

as strategy, changing risk, significant issues, etc. Describe relevant committee meetings that include the topic of cybersecurity, with specific focus on programs of work to improve maturity and reduce risk. Describe when/how/where any breaches or other cybersecurity events have been discussed.

Examples of Effective Evidence:

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-031: Cybersecurity and Technology Officer Leadership Documentation

- Job descriptions and role profiles for the Cybersecurity Officer and Technology Officer, outlining responsibilities and qualifications.
- Strategic plans and objectives developed by the Cybersecurity Officer and Technology Officer, with documented board or executive approval.
- Records of security initiatives led by these officers, including project plans, status updates, and outcomes.
- Documentation of regular updates or briefings provided to the board and senior management by these officers.
- Evidence of the performance of 360-degree reviews of the Cybersecurity Officer and Technology Officer.
- Performance evaluations or reviews of the Cybersecurity Officer and Technology Officer, assessing their effectiveness and impact.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.
- Risk management review reports that are presented to the board, including findings and recommendations.
- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.
- Training materials for board members on risk management principles and their oversight responsibilities.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GV.OV-01.03: The designated Technology Officer (e.g., CIO or CTO) regularly reports to the governing authority (e.g., the Board or one of its committees) on the status of technology use and risks within the organization.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #metrics_and_reporting | #mission_and_strategy | #policy_management | #risk_oversight | #technology_officer

Response Guidance:

The organization should have relevant oversight functions responsible to develop, present, and discuss the status of technology use and risks within the organization. The designated Technology Officer (e.g., CIO or CTO) should provide a report on the status of technology use and risks within the organization to the Board of Directors.

Describe how the organization CIO or CTO effectively manages the status of technology use and risks within the organization. Provide information on how the designated Technology Officer reports to the Board Risk Committee. Additionally, provide information regarding presentations to the Board of Directors by the designated Technology Officer, in annual or quarterly meetings, including updates such as strategy, changing risk, significant issues etc. Describe relevant committee meetings that include the topic of risk management, with specific focus on programs to work to improve maturity and reduce risk. Describe when updates in an organization's risk profile have been discussed.

Examples of Effective Evidence:

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-031: Cybersecurity and Technology Officer Leadership Documentation

- Job descriptions and role profiles for the Cybersecurity Officer and Technology Officer, outlining responsibilities and qualifications.
- Strategic plans and objectives developed by the Cybersecurity Officer and Technology Officer, with documented board or executive approval.
- Records of security initiatives led by these officers, including project plans, status updates, and outcomes.
- Documentation of regular updates or briefings provided to the board and senior management by these officers.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Evidence of the performance of 360-degree reviews of the Cybersecurity Officer and Technology Officer.
- Performance evaluations or reviews of the Cybersecurity Officer and Technology Officer, assessing their effectiveness and impact.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.
- Risk management review reports that are presented to the board, including findings and recommendations.
- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.
- Training materials for board members on risk management principles and their oversight responsibilities.

GOVERN / Oversight / Risk Management Strategy Review & Adjustment

GV.OV-02.01: The organization regularly assesses its inherent technology and cybersecurity risks and ensures that changes to the business and threat environment lead to updates to the organization's strategies, programs, risk appetite and risk tolerance.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #enterprise_risk_management | #mission_and_strategy | #risk_appetite_/_tolerance | #risk_management | #threat_management

Response Guidance:

Describe how the organization's strategies, programs, risk appetite, and risk tolerance articulate and address its inherent technology and cybersecurity risks. Describe the programs in place to address perimeter security, application security, infrastructure protection, threat environment, etc.

Describe the organization's process for identifying and tracking threats, vulnerabilities, and risks, and whether strategies, programs, risk appetite, and risk tolerance levels are updated to reflect changes in the organization's operating environment and threat environment.

Examples of Effective Evidence:

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-005: Risk Appetite Tolerance, and Strategy Alignment Documents

- Risk appetite statements approved by the board or executive management.
- Risk tolerance levels defined for different categories of risk.
- Documentation on how risk appetite influences decision-making and strategy.
- Reports on risk exposures compared to the defined risk appetite.
- Updates or revisions to risk appetite and tolerance based on changing conditions.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.
- Risk management review reports that are presented to the board, including findings and recommendations.
- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.
- Training materials for board members on risk management principles and their oversight responsibilities.

EEE-093: Risk Management Strategy and Framework Documentation

- Documentation of the organization's risk management strategy and framework, outlining risk identification, assessment, and mitigation processes.
- Records from risk management framework review sessions, including updates made to adapt to new risks or business changes.
- Risk registers or databases tracking identified risks, assessments, and mitigation actions over time.
- Stakeholder reports summarizing the state of risk management within the organization and strategic recommendations.
- External audit or consultant reviews of the risk management framework, providing independent assessments and suggestions for improvement.

EEE-094: Technology and Cybersecurity Risk Appetite Documents

- Official statements or documents defining the organization's risk appetite specifically related to technology and cybersecurity.
- Board or executive committee meeting minutes discussing and approving the risk appetite statement.
- Guidelines for aligning IT and cybersecurity initiatives with the defined risk appetite.
- Reviews or assessments of projects and initiatives to ensure they are within the organization's technology and cybersecurity risk appetite.

EEE-104: Risk Tolerance and Management Practice Integration Documentation

- Documentation of the organization's risk tolerance levels and how these are integrated into risk management practices.
- Records of risk assessments that consider the organization's risk tolerance when determining mitigation strategies.
- Reports to management and the board on risk exposures in relation to the defined risk tolerance.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Reviews of risk management practices to ensure they remain aligned with the organization's risk tolerance.

GV.OV-02.02: The organization determines and articulates how it intends to maintain an acceptable level of residual technology and cybersecurity risk as set by the governing authority (e.g., the Board or one of its committees).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #enterprise_risk_management | #program_transformation | #risk_management | #risk_response

Response Guidance:

Residual risk is the risk remaining after current controls are considered. The appropriate governing authority should determine the organization's residual risk levels and monitor outliers until risks are mitigated.

High and moderate residual technology and cybersecurity risk should be monitored until the risks are addressed or accepted as required by policy.

Provide information on how the organization maintains an acceptable level of residual risk as set by the governing authority.

Examples of Effective Evidence:

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-005: Risk Appetite Tolerance, and Strategy Alignment Documents

- Risk appetite statements approved by the board or executive management.
- Risk tolerance levels defined for different categories of risk.
- Documentation on how risk appetite influences decision-making and strategy.
- Reports on risk exposures compared to the defined risk appetite.
- Updates or revisions to risk appetite and tolerance based on changing conditions.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Risk management review reports that are presented to the board, including findings and recommendations.
- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.
- Training materials for board members on risk management principles and their oversight responsibilities.

EEE-093: Risk Management Strategy and Framework Documentation

- Documentation of the organization's risk management strategy and framework, outlining risk identification, assessment, and mitigation processes.
- Records from risk management framework review sessions, including updates made to adapt to new risks or business changes.
- Risk registers or databases tracking identified risks, assessments, and mitigation actions over time.
- Stakeholder reports summarizing the state of risk management within the organization and strategic recommendations.
- External audit or consultant reviews of the risk management framework, providing independent assessments and suggestions for improvement.

EEE-094: Technology and Cybersecurity Risk Appetite Documents

- Official statements or documents defining the organization's risk appetite specifically related to technology and cybersecurity.
- Board or executive committee meeting minutes discussing and approving the risk appetite statement.
- Guidelines for aligning IT and cybersecurity initiatives with the defined risk appetite.
- Reviews or assessments of projects and initiatives to ensure they are within the organization's technology and cybersecurity risk appetite.

GOVERN / Oversight / Risk Management Performance Measurement

GV.OV-03.01: The organization develops, implements, and reports to management and the governing body (e.g., the Board or one of its committees) key technology and cybersecurity risk and performance indicators and metrics to measure, monitor, and report actionable indicators.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #board_or_committee_oversight | #metrics_and_reporting

Response Guidance:

The organization should use technology and cybersecurity metrics to determine where weaknesses or gaps exist within their programs. The metrics can then be used to identify trends, make strategic decisions to address those trends, and allocate funding appropriately. Technology and cybersecurity metrics can facilitate decision making and improve performance. The metrics should be quantifiable, observable, and use objective data. Management should present to the Board the threats and related trends that are most prevalent and may impact the organization. Reports should address potential or

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

future risk exposure, which can help management identify how to strengthen the organization's security posture.

Provide available information on security risk reporting to the appropriate governing body (e.g., the Board or one of its committees). Describe how KRIs and KCIs are used to measure risks and controls aligned to the organization's strategy. Describe ownership of KRIs/KCIs and the review process. Provide information on how the organization's risk appetite is used to determine the risk appetite statement metrics (including technology and cybersecurity risk related KRIs) and the tolerance thresholds defined for each metric. Describe how the risk appetite profile, risk map, and top and emerging risk report, are reported to the appropriate governing body (e.g., to the Board Risk Committee at each meeting).

Examples of Effective Evidence:

EEE-051: Risk Metrics and Performance Indicator Documentation

- Key performance indicators (KPIs) and risk metrics used to measure the effectiveness of the organization's risk management program.
- Dashboards or reports that track and display collected performance indicators and risk metrics.
- Documentation of the process for collecting, analyzing, and reporting on KPIs and risk metrics.
- Historical data and trend analysis used to inform risk management decisions and strategies.
- Records of management reviews or meetings where performance indicators and risk metrics are discussed and used to drive decision making or improvements.

GV.OV-03.02: Resilience program performance is measured and regularly reported to senior executives and the governing authority (e.g., the Board or one of its committees).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #metrics_and_reporting | #resilience

Response Guidance:

Describe how the organization develops, monitors, and regularly reports on the performance of their resilience program to senior executives and the governing authority. Measures of performance and metrics are used by an organization to measure the effectiveness of the organization's ability to recover from a significant disruption and resume critical operations or operate within an degraded and disrupted operational environment.

Provide information on how an organization establishes standards and processes with defined performance indicators and/or metrics that can be used to measure and monitor the ability to timely recovery and resumption of operations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-059: Enterprise and Cyber Resilience Policy Documentation

- Official enterprise resilience strategy documents that outline the organization's approach to achieving and maintaining resilience.
- Cyber resilience policy documents that specify the measures and controls in place to protect against cyber threats.
- Board presentations and approvals related to the resilience strategy and cyber resilience policies.
- Reports from resilience assessments, including gap analyses and recommendations for improvement.

GOVERN / Supply Chain Risk Management / Supply Chain Risk Management Program

GV.SC-01.01: The organization maintains a third-party risk management strategy and program to identify and manage the risks associated with third parties throughout their lifecycles in a timely manner, including in support of sector-critical systems and operations, to ensure alignment within risk appetite.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #critical_infrastructure | #risk_appetite_/_tolerance | #risk_management | #third_party_risk_management | #supply_chain_management

Response Guidance:

The organization's policies, plans, and procedures should include processes for inventorying third parties and strategies for identifying and managing risks. The organization's policies, plans, and procedures should include assessing the inherent risk and criticality of a third party to the organization and the processes to manage that risk over the lifecycle of the relationship.

Provide information on the established policies, plans, and procedures used to identify and manage cyber risks associated with third parties throughout their lifecycles in a timely manner, including sector-critical systems and operations. Describe or provide information on how the organization assesses cyber risks associated with external dependences through security questionnaires, business impact analysis, or other assessment.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-018: Supplier Evaluation, Onboarding, and Due Diligence Documentation

- Checklists and criteria used for evaluating potential suppliers, including security and resilience factors.
- Due diligence reports for key suppliers, including assessments of their financial stability and operational resilience.
- Agreements that include clauses related to ongoing monitoring and evaluation of supplier performance.
- Records of supplier selection meetings, including rationale for decisions and any identified risks.
- Supplier onboarding process documentation, highlighting security and resilience requirements.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

GV.SC-01.02: The organization regularly assesses the risk of its ongoing use of third parties in aggregate, considering factors such as critical service dependencies, vendor concentration, geographical/geopolitical exposure, fourth-party impacts, and financial sector co-dependencies.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #business_impact_analysis | #critical_infrastructure | #dependency_management | #due_diligence | #fourth_party | #third_party_risk_management | #vendor_management | #supply_chain_management

Response Guidance:

Provide information on the organization's policies and procedures used to assess third party risk in aggregate, i.e., not with respect to any individual supplier or vendor. Describe the third party risk program including strategies and analysis of critical third parties. Provide information on the review and analysis of the organization's reliance of third party service providers, the analysis should include

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

considerations of critical service dependencies, vendor concentration, geographical/geopolitical exposure, fourth-party impacts, and financial sector co-dependencies.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-018: Supplier Evaluation, Onboarding, and Due Diligence Documentation

- Checklists and criteria used for evaluating potential suppliers, including security and resilience factors.
- Due diligence reports for key suppliers, including assessments of their financial stability and operational resilience.
- Agreements that include clauses related to ongoing monitoring and evaluation of supplier performance.
- Records of supplier selection meetings, including rationale for decisions and any identified risks.
- Supplier onboarding process documentation, highlighting security and resilience requirements.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GOVERN / Supply Chain Risk Management / Third Party Roles & Responsibilities

GV.SC-02.01: The organization clearly defines, and includes in contractual agreements, the division of cybersecurity and technology risk management responsibilities between the organization and its third parties (e.g., a Shared Responsibilities Model).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #contract_management | #risk_management | #roles_and_responsibilities | #third_party_risk_management | #vendor_management | #supply_chain_management

Response Guidance:

Management must require third-party service providers by contract to implement appropriate measures designed to meet the organization's minimum cybersecurity requirements and the objectives of regulatory guidelines.

Provide detail on how the organization establishes and maintains contracts with third-party service providers to define the risk management roles and responsibilities between the organization and service provider, including the division of cybersecurity and technology risk management. Review existing contract and boilerplate language to confirm whether additional contractual language is required or should be expanded upon. Provide information on how the organization establishes a shared responsibilities model or similar mechanism to ensure that all appropriate responsibilities are documented, managed, unambiguously assigned, and shared responsibilities are clear between a customer and third party service provider.

Examples of Effective Evidence:

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

GOVERN / Supply Chain Risk Management / Supply Chain Risk Management Integration

GV.SC-03.01: The organization's third-party risk management strategy and program aligns with and supports its enterprise, technology, cybersecurity, and resilience risk management frameworks and programs.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #mission_and_strategy | #risk_management | #third_party_risk_management | #supply_chain_management

Response Guidance:

Organizations are reliant on third parties throughout the enterprise, and within multiple program areas (e.g., technology, cybersecurity, and resilience). The organization's third-party risk management strategy and program should be aligned to the organization's risk management frameworks and programs as third parties should be considered as an extension of the organization due to their involvement.

Describe how the organization has integrated its third-party risk management strategy and program supports and aligns with the enterprise, technology, cyber, and resilience risk management frameworks and programs. For example, for cyber risk alignment, the organization may include standard language to contracts with third-parties related to cyber risk.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

GOVERN / Supply Chain Risk Management / Supplier Identification & Prioritization

GV.SC-04.01: The organization regularly identifies, inventories, and risk-ranks third-party relationships that are in place, and addresses any identified relationships that were established without formal approval.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #dependency_management | #third_party_risk_management | #supply_chain_management

Response Guidance:

The organization should identify all third-party service providers (e.g., core processing, online and mobile banking, settlement activities, disaster recovery services, cloud service providers, application programming interfaces (API), and other emerging technologies) and categorize them with respect to risk.

Describe how the organization's third-party risk management program and process identifies, tracks, and inventories third-party relationships that are in place, including those relationships that were established without formal approval. One means to detect new relationships which bypassed the formal approval process is to reconcile the accounts payable with a listing of managed third-party vendors. Procedures can also be implemented to disallow procurement of certain vendor services without the approval of the security and/or technology functions. Highlight the process and any tools used. Understanding what third-party relationships are in place including those that have been established without formal approval can be useful for identifying potential risks and threats as well as aiding response activities during an information security event.

Examples of Effective Evidence:

EEE-010: IT Asset Management and Business Function Mapping Documentation

- Inventory list of IT assets, including hardware, software, and data.
- Business function catalog that maps key assets to their corresponding business process.
- Asset ownership and stewardship records indicating who is responsible for specific assets.
- Lifecycle management records for assets, showing purchase dates, warranty periods, and disposal information.
- Integration diagrams showing how assets interact within the business's technology ecosystem.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-018: Supplier Evaluation, Onboarding, and Due Diligence Documentation

- Checklists and criteria used for evaluating potential suppliers, including security and resilience factors.
- Due diligence reports for key suppliers, including assessments of their financial stability and operational resilience.
- Agreements that include clauses related to ongoing monitoring and evaluation of supplier performance.
- Records of supplier selection meetings, including rationale for decisions and any identified risks.
- Supplier onboarding process documentation, highlighting security and resilience requirements.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

GOVERN / Supply Chain Risk Management / Third Party Incident Management Integration

GV.SC-08.01: The organization's resilience strategy, plans, tests, and exercises incorporate its external dependencies and critical business partners.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #business_impact_analysis | #dependency_management | #mission_and_strategy | #review_assessment_and_testing | #threat_landscape

Response Guidance:

The organization’s third-party risk management strategy should be incorporated into the resilience strategy. Describe how the organization has incorporated its third parties and critical business partners into its resilience (e.g., incident response, business continuity, and disaster recovery) strategy, plans, tests, and exercises.

Examples of Effective Evidence:

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.
- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-015: Sector-Wide Dependency and Impact Analysis Documentation

- Analysis reports detailing the dependencies within the organization's sector and potential vulnerabilities.
- Tools or software used to evaluate the criticality of external partners and suppliers.
- Summaries from workshops and exercises aimed at understanding the sector-wide impact of external disruptions.
- Reports on how regulatory changes could affect critical external dependencies.
- Real-time dashboards for monitoring geopolitical events that may impact the sector.

GOVERN / Supply Chain Risk Management / Supply Chain Security Practice Integration

GV.SC-09.01: Consideration is specifically given to the implications of organizational third-party dependence, requirements, contracts, and interactions in the design, operation, monitoring, and improvement of policies, procedures, and controls to ensure the fulfillment of business requirements within risk appetite.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #contract_management | #dependency_management | #policy_management | #risk_appetite_/_tolerance | #third_party_risk_management | #supply_chain_management

Response Guidance:

Describe how the organization evaluates their third-party dependence, requirements, contracts, and interactions in the design, operation, monitoring, and improvement of policies, procedures, and controls.

Provide information on the third-party risk management and vendor management policies, plans, and procedures. Describe or provide information on how the organization assesses the implication of changes to business operation requirements involving third-party dependencies, requirements, and interactions. Detail how the organization updates contracts and boilerplates to align with the businesses risk appetite and business requirements

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

GOVERN / Independent Risk Management Function / Independent Risk Management Function

GV.IR-01.01: The organization's enterprise-wide technology and cybersecurity risk management frameworks align with and support an independent risk management function that provides assurance that the frameworks are implemented consistently and as intended.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #enterprise_risk_management | #risk_management

Response Guidance:

Enterprise risk management objectives and actions encompass technology and cybersecurity risk mitigation and acceptance decisions. These decisions align with overall risk tolerance and enable, rather than limit or inhibit, business objectives.

Describe how the operational risk management framework and the three lines of defense pertain to an independent risk management function that provides assurance that the technology and cybersecurity risk management framework is implemented as intended (e.g., through credible challenge). Describe how the 2LoD oversees the controls implemented by the 1LoD to ensure controls are operating effectively. Provide examples of 3LoD or other independent assurance over

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

the technology and cybersecurity risk management framework, including documentation and evidence of review of credible challenge.

Examples of Effective Evidence:

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

GV.IR-01.02: The independent risk management function has sufficient independence, stature, authority, resources, and access to the governing body (e.g., the Board or one of its committees), including reporting lines, to ensure consistency with the organization's risk management frameworks.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #board_or_committee_oversight | #enterprise_risk_management | #risk_management | #risk_oversight

Response Guidance:

Describe the operational risk management framework and how the three lines of defense create and allow an independent risk management function that has sufficient independence, stature, authority, resources, and access to the appropriate governing body (e.g., the Board or one of its committees), including reporting lines, to ensure consistency with the organization's cybersecurity risk management framework. Provide examples of independence.

Describe reporting structures to demonstrate independence and explain how businesses are supported (e.g., being provided guidance/oversight on the related risks and controls, including evaluation of control monitoring activity).

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

GV.IR-01.03: The independent risk management function has an understanding of the organization's structure, technology and cybersecurity strategies and programs, and relevant risks and threats.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #enterprise_risk_management | #mission_and_strategy | #risk_management | #threat_management

Response Guidance:

Describe how the operational risk management framework and how the three lines of defense create an independent risk management function that has understanding of the organization's structure, technology strategy, cybersecurity program, and relevant risks and threats. Provide examples of how the various lines of defense understanding of the programs in place. Describe how both the 2LoD and 3LoD possesses or has access to a reasonable and appropriate level of cybersecurity skills to ensure credible challenge and control implementation. For example, cybersecurity skills capability frameworks and training, reporting, and observations.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

GOVERN / Independent Risk Management Function / Independent Risk Management Evaluation

GV.IR-02.01: The independent risk management function regularly evaluates the appropriateness of the technology and cybersecurity risk management programs to the organization's risk appetite and inherent risk environment

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #enterprise_risk_management | #risk_appetite_/_tolerance | #risk_management

Response Guidance:

Describe how 2LoD within the risk department is separate from the business/function lines within the organization. Provide information on how 2LoD supports the organization's businesses/functions by providing guidance/oversight on the related risks and controls, including evaluation of control monitoring activity.

Describe how the 2LoD possesses or has access to a reasonable and evalutes the appropriate level of cybersecurity skills to ensure credible challenge and control implementation. Describe how the risk appetite profile is used to monitor the risk appetite statement metrics (including technology and cybersecurity risk related key risk indicators (KRIs)) against the appetite and tolerance thresholds defined for each metric. Describe how the metrics include trends of control improvements over time.

Examples of Effective Evidence:

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-005: Risk Appetite Tolerance, and Strategy Alignment Documents

- Risk appetite statements approved by the board or executive management.
- Risk tolerance levels defined for different categories of risk.
- Documentation on how risk appetite influences decision-making and strategy.
- Reports on risk exposures compared to the defined risk appetite.
- Updates or revisions to risk appetite and tolerance based on changing conditions.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GV.IR-02.02: The independent risk management function regularly assesses the organization's controls and cybersecurity risk exposure, identifies opportunities for improvement based on assessment results, and recommends program improvements

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #enterprise_risk_management | #program_transformation | #review_assessment_and_testing | #risk_management | #improvements

Response Guidance:

Provide information on how the independent risk management function, as part of 2LoD, provides oversight of cybersecurity controls and risk exposure through a risk and control assessment process. Describe how the independent risk management function provides guidance/oversight on the related risks and controls, including the evaluation of control monitoring activity. Describe the annual cybersecurity assessment process utilizing the Profile and how an overall maturity rating for each of the seven Profile Functions is determined within the assessment. Where the organization does not have a particular control in place, describe how self-identified issues are organized appropriately to track remediation. Describe the number/types of reports, including any dashboards which provide details on risks and threats identified, mitigating actions proposed and their status along with updates on the deliverables, and applicable program and control improvements being delivered. Document to whom reports are provided (e.g., committees, board, management meetings).

Examples of Effective Evidence:

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.
- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.
- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

GOVERN / Independent Risk Management Function / Independent Risk Management Reporting

GV.IR-03.01: The independent risk management function reports to the governing authority (e.g., the Board or one of its committees) and to the designated risk management officer within the organization on the implementation of the technology and cybersecurity risk management frameworks throughout the organization and its independent assessment of risk posture.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #board_or_committee_oversight | #enterprise_risk_management | #metrics_and_reporting | #risk_management | #risk_oversight

Response Guidance:

Provide information on how the independent risk management function, as part of 2LoD, reports to the appropriate governing authority and to the appropriate risk management officer within the organization.

When significant discrepancies in a business unit's technology or cybersecurity risk assessment exists within the organization, a process to elevate the discrepancies to the designated risk management office and/or Board's attention should be in place.

Describe how technology and cyber program updates are provided in governance meetings and whether there is a standing agenda item on cybersecurity internal/external incidents. Include other types of meetings where cyber incidents/events or the risk appetite of the organization are discussed. Describe tracking/reporting of audit remediation, assessment issues, etc.

Examples of Effective Evidence:

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.
- Risk management review reports that are presented to the board, including findings and recommendations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.
- Training materials for board members on risk management principles and their oversight responsibilities.

GOVERN / Independent Audit Function / Independent Audit Compliance Assessment

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

GV.AU-01.01: The organization has an independent audit function (i.e., internal audit group or external auditor) that follows generally accepted audit practices and approved audit policies and procedures.

Subject Tags: #audit_planning_and_testing | #organizational_structure

Response Guidance:

A well-planned, properly structured independent audit program is essential to evaluate risk management practices, internal control systems, and compliance with corporate policies concerning cyber and IT-related risks at organizations of every size and complexity. Describe how internal audit's role as the third line of defense is independent of the 1LoD and 2LoD. Describe how the independence of internal audit from day-to-day line management responsibility is fundamental to the organization's ability to deliver objective coverage of all parts of the group.

If an external audit organization is used, accepted audit practices, policies, and procedures should be established and communicated to ensure guidelines are followed to test if an organization's controls in place are designed and operate effectively.

Examples of Effective Evidence:

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

GV.AU-01.02: The organization has an independent audit plan that provides for the evaluation of technology and cybersecurity risk, including compliance with the approved risk management framework, policies, and processes for technology, cybersecurity, and resilience; and how well the organization adapts to the evolving risk environment while remaining within its stated risk appetite and tolerance.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #audit_planning_and_testing | #risk_appetite_/_tolerance | #risk_oversight

Response Guidance:

Effective audit programs are risk-focused and promote sound IT controls across the organization. The risk management function is an essential part of corporate governance. Complex organizations should have a more robust risk management function. There should be an independent review and evaluation to validate its effectiveness. Describe how the independent review of technology and cybersecurity risk is covered by internal audit teams through various audits. Audits should address the effectiveness of the 1LoD and 2LoD activities for managing and controlling technology and cybersecurity risk.

Provide information and evidence on how IT audit works closely with other areas of audit (e.g., operational risk audit). Describe what is being assessed by audit in addition to any themed audits which can focus on specific technologies or layers of infrastructure (e.g., access, databases, core technical platforms, internet banking, email systems, internal and external connectivity, cyber detection, and prevention). Audits that cover security control and oversight processes (e.g., lines of defense, change management, access recertification, authentication) which include technology, cybersecurity, and resilience as key risk coverage should be included as well as stand-alone cyber related audits.

Provide information and evidence on all areas of audit that may assess the wider aspects of information security risk, including the organization and management of the information security risk function, data and business continuity risk, the business-wide effectiveness of associated standards and general controls, and the risk appetite of security areas.

Examples of Effective Evidence:

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

EEE-098: Customer Data Privacy and Compliance Documents

- Privacy policies and procedures that detail how customer data is protected and used in compliance with relevant laws and regulations.
- Records of privacy compliance audits, including findings and corrective actions taken.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of customer consent and data handling practices, demonstrating adherence to privacy principles.
- Training records for staff on data privacy regulations and customer data handling procedures.
- Incident logs related to customer data privacy, including any breaches and the organization's response.

GV.AU-01.03: The independent audit function tests technology management, cybersecurity, incident response, and resilience policies and controls.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #audit_planning_and_testing | #review_assessment_and_testing

Response Guidance:

An effective audit program evaluates risk management practices, internal control systems, and compliance with corporate policies concerning IT-related risks. Technology management, cybersecurity, incident response, and resilience controls are an integral part of the organization's information security control environment, and like all control systems, independent audit is responsible for validating that they are effective and commensurate with the organization's risk profile.

Describe how controls and policies are assessed as part of internal audit's charter and security-related audits.

Describe when/how the audit schedule is published/approved. Describe how the 3LoD possesses or has access to a reasonable and appropriate level of cybersecurity skills to ensure credible challenge and control implementation.

Examples of Effective Evidence:

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

GV.AU-01.04: The independent audit function evaluates and tests third-party risk management policies and controls, identifies weaknesses and gaps, and recommends improvements to senior management and the governing authority (e.g., the Board or one of its committees).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #metrics_and_reporting | #policy_management | #review_assessment_and_testing | #risk_management | #risk_oversight | #third_party_risk_management | #audit_planning_and_testing | #supply_chain_management

Response Guidance:

Independent audits should be used to evaluate and test the effectiveness of third-party risk management program. The audit process should validate that current policies and controls are in fact working properly, as well as assess whether the organization has the appropriate level of expertise to effectively manage these controls. The audit report should identify weaknesses and gaps in existing policies and controls.

Describe how the independent audit function performs third-party risk management audits periodically. Responses should provide information about how the independent audit function raises audit issues when necessary to senior management and the governing authority, how management addresses the issues, and how internal audit tracks issues through resolution. Describe how the organization conducts review of third-party risk management policies and controls to determine if gaps exist and recommends improvements to work towards self-improvement of the program.

Examples of Effective Evidence:

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

GV.AU-01.05: An independent audit function assesses compliance with applicable laws and regulations.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #audit_planning_and_testing | #review_assessment_and_testing

Response Guidance:

Describe how internal audit identifies applicable laws and regulations in its auditable entities and how the planning process within each audit identifies which laws and regulations will be part of the audit scope. Testing of compliance with laws and regulations are completed per the audit plan.

Examples of Effective Evidence:

EEE-007: Legal, Regulatory, and Compliance Management Documentation

- Compliance audit reports for relevant laws and regulations (e.g., GDPR, HIPAA).
- Documentation of legal advice received on cybersecurity matters, to include determinations of incident materiality.
- Records of regulatory filings and notices related to IT and cybersecurity.
- Updates to policies and procedures in response to legal and regulatory changes.
- Training records on legal and regulatory requirements for IT staff.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

EEE-098: Customer Data Privacy and Compliance Documents

- Privacy policies and procedures that detail how customer data is protected and used in compliance with relevant laws and regulations.
- Records of privacy compliance audits, including findings and corrective actions taken.
- Documentation of customer consent and data handling practices, demonstrating adherence to privacy principles.
- Training records for staff on data privacy regulations and customer data handling procedures.
- Incident logs related to customer data privacy, including any breaches and the organization's response.

GOVERN / Independent Audit Function / Independent Audit Procedures

GV.AU-02.01: A formal process is in place for the independent audit function to review and update its procedures and audit plans regularly or in response to changes in relevant standards, the technology environment, or the business environment.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #audit_planning_and_testing | #compliance | #industry_standards | #policy_management

Response Guidance:

Provide information on how internal audit reviews and updates its assessment of cyber risks based on its continuous monitoring process and audit universe coverage. Describe how audit procedures and audit plans are adjusted to ensure sufficient audit coverage.

The independent audit function should not be limited to the major activities and operations of the organization and should recognize the organization’s role in the financial sector (e.g., interdependencies within the sector).

Given the evolving threat landscape across the financial sector, the audit risk assessment should address potential impacts and analyze whether additional procedures are necessary to validate appropriate controls are in place.

Examples of Effective Evidence:

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

GV.AU-02.02: A formal process is in place for the independent audit function to update its procedures and audit plans based on changes to the organization's risk appetite, risk tolerance, threat environment, and evolving risk profile.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #audit_planning_and_testing | #policy_management | #risk_appetite_/_tolerance

Response Guidance:

An effective risk-based auditing program will cover all of the organization's major activities and reflect the overall risk profile. The risk appetite statement serves as the basis to determine whether risk acceptance decisions are within the organization's acceptable risk tolerance range. Risk tolerance levels can change based on changes in the organization's operating environment and threat landscape. Therefore, it is important that the independent audit function regularly reviews the organization's risk appetite statements.

Describe how internal audit regularly verifies, and if necessary, updates its assessment of risks based on its continuous monitoring process. When necessary, describe how the independent audit function adjusts the audit procedures and plans to ensure sufficient audit coverage.

Examples of Effective Evidence:

EEE-005: Risk Appetite Tolerance, and Strategy Alignment Documents

- Risk appetite statements approved by the board or executive management.
- Risk tolerance levels defined for different categories of risk.
- Documentation on how risk appetite influences decision-making and strategy.
- Reports on risk exposures compared to the defined risk appetite.
- Updates or revisions to risk appetite and tolerance based on changing conditions.

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

EEE-104: Risk Tolerance and Management Practice Integration Documentation

- Documentation of the organization's risk tolerance levels and how these are integrated into risk management practices.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

- Records of risk assessments that consider the organization's risk tolerance when determining mitigation strategies.
- Reports to management and the board on risk exposures in relation to the defined risk tolerance.
- Reviews of risk management practices to ensure they remain aligned with the organization's risk tolerance.

GOVERN / Independent Audit Function / Independent Audit Reporting

GV.AU-03.01: The independent audit function reviews technology and cybersecurity practices and identifies weaknesses and gaps.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #audit_planning_and_testing

Response Guidance:

Independent audits should be used to evaluate the effectiveness of an organization's IT control environment. The audit process should validate that current security controls are in fact working properly, as well as assess whether the organization has the appropriate level of expertise to effectively manage these security controls. The audit report should identify gaps in existing security capabilities and expertise.

Describe how the independent audit function performs technology and cybersecurity related audits according to its annual plan. Include information about how the independent audit function raises audit issues when necessary, how management addresses the issues, and how internal audit tracks issues through resolution. Describe how issues that need immediate action are raised to management. Describe how the internal audit process/scope includes an assessment of security capabilities/expertise, is documented in the results, and identified in the final report.

Examples of Effective Evidence:

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

GV.AU-03.02: The independent audit function tracks identified issues and corrective actions from internal audits and independent testing/assessments to ensure timely resolution.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #audit_planning_and_testing

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Audit results identify weaknesses in an organization's cybersecurity program. Management should develop corrective actions to address identified weaknesses.

Describe how all audit issues are tracked by the independent audit function and follow ups are performed to ensure timely closure by management. Describe concept/benefits of continuous monitoring to highlight any concerns within various programs of work. Provide information on how internal audit also performs validation to ensure design and operating effectiveness prior to formal closure of any audit issue. Describe tracking of status on risk in finding remediation and how it is provided to senior management. Provide information on how past due findings are escalated.

Examples of Effective Evidence:

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

GV.AU-03.03: The independent audit function reports to the governing authority (e.g., the Board or one of its committees) within the organization, including when its assessment differs from that of the organization, or when risk tolerance has been exceeded in any part of the organization.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #audit_planning_and_testing | #board_or_committee_oversight | #metrics_and_reporting | #review_assessment_and_testing | #risk_appetite_/_tolerance | #risk_management | #risk_oversight

Response Guidance:

Describe how the independent audit function reports to the governing authority (e.g., Board Audit Committee) on cyber risks, including current threats. When significant discrepancies in a business unit's cybersecurity risk assessment exists within the organization, a process to elevate the discrepancies to management's or the Board's attention should be in place. Processes should be in place to notify the appropriate governing authority if the risk tolerance is exceeded.

Examples of Effective Evidence:

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-104: Risk Tolerance and Management Practice Integration Documentation

- Documentation of the organization's risk tolerance levels and how these are integrated into risk management practices.
- Records of risk assessments that consider the organization's risk tolerance when determining mitigation strategies.
- Reports to management and the board on risk exposures in relation to the defined risk tolerance.
- Reviews of risk management practices to ensure they remain aligned with the organization's risk tolerance.

IDENTIFY / Asset Management / Hardware Inventory

ID.AM-01.01: The organization maintains a current and complete asset inventory of physical devices, hardware, and information systems.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #asset_classification_and_criticality | #asset_inventory | #asset_management | #asset_ownership | #critical_infrastructure | #physical_infrastructure

Response Guidance:

An asset inventory is a comprehensive record of an organization’s hardware, software (e.g., physical and virtual servers, operating systems, and business applications), and data repositories (e.g., customer information files or storage area network). The current inventory system of record is updated as frequently as necessary for the organization to successfully manage downstream processes reliant on an accurate asset inventory. However, management should update the asset inventory at least annually, or more frequently depending on risk, and should identify new assets as well as those relocated to another site.

For this Diagnostic Statement, describe the processes and tools related to maintaining a complete asset inventory of physical devices, hardware, and information systems. Include how accountability for data within the asset inventory is managed, how the inventory is updated to maintain current information, as well as roles and responsibilities.

Examples of Effective Evidence:

EEE-010: IT Asset Management and Business Function Mapping Documentation

- Inventory list of IT assets, including hardware, software, and data.
- Business function catalog that maps key assets to their corresponding business process.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Asset ownership and stewardship records indicating who is responsible for specific assets.
- Lifecycle management records for assets, showing purchase dates, warranty periods, and disposal information.
- Integration diagrams showing how assets interact within the business's technology ecosystem.

EEE-011: External Dependencies and Risk Assessment Documents

- Diagrams of network architecture showing connections to external systems and services.
- Contracts and service level agreements (SLAs) with key vendors and service providers.
- Risk assessments of external dependencies highlighting potential impact on business operations.
- Documentation of alternative vendors and backup resources in case of primary vendor failure.
- Incident reports related to external dependencies, including response and resolution details.

EEE-034: Asset Management and Inventory Oversight Documentation

- Asset management policies that outline the processes and data requirements for tracking, maintaining, and securing organizational assets.
- Inventory lists or databases of assets, including hardware, software, data, and intellectual property, with assigned custodians or owners.
- Change logs or records of asset transfers, disposals, and acquisitions.
- Technical documentation and configuration of automated inventory discovery and management tools.
- Reports from periodic asset audits or reviews, confirming the accuracy of the inventory and compliance with the policy.
- Documentation of asset classification and labeling, indicating the criticality and sensitivity of assets.

EEE-056: Operational Technology and IoT Security Documentation

- Security policies and procedures specific to operational technology (OT) and Internet of Things (IoT) devices.
- Inventory lists of OT and IoT devices, including security features and firmware versions.
- Risk assessments for OT and IoT devices, identifying potential vulnerabilities and mitigation strategies.
- Configuration standards for various types of OT and IoT devices (e.g., default password reset).
- Incident response plans that include protocols for addressing security incidents involving OT and IoT devices.
- Documentation of security patches and updates applied to OT and IoT devices, along with testing results.

EEE-065: Asset Management and Custodianship Documentation

- Asset management policies that outline the procedures for asset custodianship, including accountability for asset security and maintenance.
- Records of asset assignments to custodians, including acknowledgment of responsibilities.
- Audit trails showing the tracking and verification of asset location, status, and custodianship.
- Reports from periodic reviews of asset management practices and custodian performance.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

IDENTIFY / Asset Management / Software, Services, & Systems Inventory

ID.AM-02.01: The organization maintains a current and complete inventory of software platforms, business applications, and other software assets (e.g., virtual machines and virtual network devices).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #asset_classification_and_criticality | #asset_inventory | #asset_management | #asset_ownership | #critical_infrastructure | #physical_infrastructure

Response Guidance:

An asset inventory is a comprehensive record of an organization's software platforms, business applications and other software (e.g., physical and virtual servers, operating systems, and business applications), and data repositories (e.g., customer information files or storage area network). The current inventory system of record is updated as frequently as necessary for the organization to successfully manage downstream processes reliant on an accurate asset inventory. However, management should update the asset inventory at least annually, or more frequently depending on risk, and should identify new assets as well as those relocated to another site.

Describe the processes and tools related to maintaining a complete inventory of software platforms and business applications (refer to ID.AM-01.01 for asset inventory of physical devices, hardware, and information systems). The inventory should be integrated into the systems management lifecycle (through to destruction) and reconciled with other systems to ensure accuracy. The record will typically include the device type, and software version and end of support date to help the organization manage software updates, patches, and replacements. It will typically include the owner or responsible group, location/region, and the criticality or sensitivity level. It may also include the software utilized and data held at third parties. Firmware may be addressed as a component of this Diagnostic Statement or within the organization's set of configuration management controls.

Examples of Effective Evidence:

EEE-010: IT Asset Management and Business Function Mapping Documentation

- Inventory list of IT assets, including hardware, software, and data.
- Business function catalog that maps key assets to their corresponding business process.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Asset ownership and stewardship records indicating who is responsible for specific assets.
- Lifecycle management records for assets, showing purchase dates, warranty periods, and disposal information.
- Integration diagrams showing how assets interact within the business's technology ecosystem.

EEE-034: Asset Management and Inventory Oversight Documentation

- Asset management policies that outline the processes and data requirements for tracking, maintaining, and securing organizational assets.
- Inventory lists or databases of assets, including hardware, software, data, and intellectual property, with assigned custodians or owners.
- Change logs or records of asset transfers, disposals, and acquisitions.
- Technical documentation and configuration of automated inventory discovery and management tools.
- Reports from periodic asset audits or reviews, confirming the accuracy of the inventory and compliance with the policy.
- Documentation of asset classification and labeling, indicating the criticality and sensitivity of assets.

IDENTIFY / Asset Management / Network Communications & Data Flows

ID.AM-03.01: The organization maintains current maps of network resources, mobile resources, external connections, network-connected third parties, and network data flows.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #asset_inventory | #data_flow | #network_diagrams | #remote_access

Response Guidance:

To ensure appropriate network security, organizations should maintain accurate network and data flow diagrams that identify hardware, software, and network components, mobile components, internal and external connections, and types of information passed between systems to facilitate the development of a defense-in-depth security architecture. Management should be able to produce a visual depiction (e.g., diagram or topology map) of all external vendor or third-party connections. This could be a stand-alone document or part of the overall network topology.

Provide information related to the organization’s asset inventory that demonstrates the inventory includes maps of network resources as well as connections with external and mobile resources. A connection may be any internal or external connection. Examples include wireless, VPN, third-party service providers, network segments, or leased lines. Provide information on controls in place to ensure proper authentication and authorization to access organizational assets such as VPN devices, routers, external network resources, and wireless technologies.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-011: External Dependencies and Risk Assessment Documents

- Diagrams of network architecture showing connections to external systems and services.
- Contracts and service level agreements (SLAs) with key vendors and service providers.
- Risk assessments of external dependencies highlighting potential impact on business operations.
- Documentation of alternative vendors and backup resources in case of primary vendor failure.
- Incident reports related to external dependencies, including response and resolution details.

EEE-056: Operational Technology and IoT Security Documentation

- Security policies and procedures specific to operational technology (OT) and Internet of Things (IoT) devices.
- Inventory lists of OT and IoT devices, including security features and firmware versions.
- Risk assessments for OT and IoT devices, identifying potential vulnerabilities and mitigation strategies.
- Configuration standards for various types of OT and IoT devices (e.g., default password reset).
- Incident response plans that include protocols for addressing security incidents involving OT and IoT devices.
- Documentation of security patches and updates applied to OT and IoT devices, along with testing results.

EEE-076: Network Infrastructure and Access Control Documentation

- Network architecture diagrams that detail the infrastructure layout and access control points.
- Configuration management records for network devices, demonstrating the implementation of access controls.
- Audit logs and reports verifying compliance with network access policies and procedures.
- Incident response records showing the effectiveness of network access controls in mitigating unauthorized access.

IDENTIFY / Asset Management / Supplier Services Inventory

ID.AM-04.01: Hardware, software, and data assets maintained by or located at suppliers or other third parties are included in asset management inventories and lifecycle management processes as required for effective management and security.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #asset_classification_and_criticality | #asset_inventory | #asset_management | #asset_ownership | #critical_infrastructure | #data_lifecycle | #physical_infrastructure

Response Guidance:

Hardware, software, and data assets maintained by or located at suppliers or other third parties (e.g., remote access from personally owned devices, privately owned computing and communications devices, cloud services, etc.) are included in the organization's asset management inventory and

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

lifecycle processes as required for effective management and security. Provide information related to the inventory that demonstrates the inventory includes the key characteristics of external information systems and who manages them (e.g., vendor, contractor, end user, etc.).

Examples of Effective Evidence:

EEE-010: IT Asset Management and Business Function Mapping Documentation

- Inventory list of IT assets, including hardware, software, and data.
- Business function catalog that maps key assets to their corresponding business process.
- Asset ownership and stewardship records indicating who is responsible for specific assets.
- Lifecycle management records for assets, showing purchase dates, warranty periods, and disposal information.
- Integration diagrams showing how assets interact within the business's technology ecosystem.

EEE-011: External Dependencies and Risk Assessment Documents

- Diagrams of network architecture showing connections to external systems and services.
- Contracts and service level agreements (SLAs) with key vendors and service providers.
- Risk assessments of external dependencies highlighting potential impact on business operations.
- Documentation of alternative vendors and backup resources in case of primary vendor failure.
- Incident reports related to external dependencies, including response and resolution details.

EEE-023: Third Party Technology Security Assessment and Compliance Documents

- Assessment reports for third party software and technology, including security reviews and compliance checks.
- Documentation of the criteria and standards used for technology assessments.
- Change logs for external software, indicating how updates and patches are managed.
- Reports from third party vulnerability and security evaluation scanning services
- Vendor security certifications or attestations, such as SOC 2 reports or ISO certifications.
- Records of security testing, such as penetration tests or vulnerability scans, performed on third-party technologies.

EEE-034: Asset Management and Inventory Oversight Documentation

- Asset management policies that outline the processes and data requirements for tracking, maintaining, and securing organizational assets.
- Inventory lists or databases of assets, including hardware, software, data, and intellectual property, with assigned custodians or owners.
- Change logs or records of asset transfers, disposals, and acquisitions.
- Technical documentation and configuration of automated inventory discovery and management tools.
- Reports from periodic asset audits or reviews, confirming the accuracy of the inventory and compliance with the policy.
- Documentation of asset classification and labeling, indicating the criticality and sensitivity of assets.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-065: Asset Management and Custodianship Documentation

- Asset management policies that outline the procedures for asset custodianship, including accountability for asset security and maintenance.
- Records of asset assignments to custodians, including acknowledgment of responsibilities.
- Audit trails showing the tracking and verification of asset location, status, and custodianship.
- Reports from periodic reviews of asset management practices and custodian performance.

IDENTIFY / Asset Management / Asset Protection Prioritization

ID.AM-05.01: The organization establishes and maintains risk-based policies and procedures for the classification of hardware, software, and data assets based on sensitivity and criticality.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #asset_classification_and_criticality | #asset_inventory | #asset_management | #business_impact_analysis | #policy_management

Response Guidance:

The organization should have policies and procedures to govern the inventory and classification of hardware, software and data assets.

Describe the approved policies and procedures related to data governance and classification and related regulatory requirements (e.g., privacy requirements, transaction reporting, etc.). Provide information on how these are evaluated, maintained, and inventoried. The organization should classify and prioritize their hardware, software, and data assets according to their sensitivity and criticality. Sensitivity and criticality of an asset should be determined depending on the information it contains and its role in critical business functions. Sensitivity and criticality should consider the organization's resilience requirements.

Examples of Effective Evidence:

EEE-041: Data Governance and Retention Policy Documentation

- Data governance framework documents that outline roles, responsibilities, and processes for managing organizational data.
- Data retention schedules and policies specifying how long different types of data should be kept and the procedures for data disposal.
- Audit reports demonstrating compliance with data management and retention policies.
- Documentation of automated and manual processes used to implement data retention requirements.
- Training records for staff on data governance practices and data handling procedures.
- Documentation of data classification schemes used to manage data based on its sensitivity and importance.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-045: Data Governance and Lifecycle Management Policy Documentation

- Data governance charters or policies that define the management of data throughout its lifecycle.
- Procedures and controls for data creation, storage, usage, archiving, and destruction.
- Documentation of data lifecycle workflows, including roles involved at each stage.
- Records of data quality assessments and data cleansing activities.
- Reports on compliance with legal and regulatory requirements related to data lifecycle management.

EEE-065: Asset Management and Custodianship Documentation

- Asset management policies that outline the procedures for asset custodianship, including accountability for asset security and maintenance.
- Records of asset assignments to custodians, including acknowledgment of responsibilities.
- Audit trails showing the tracking and verification of asset location, status, and custodianship.
- Reports from periodic reviews of asset management practices and custodian performance.

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.
- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

ID.AM-05.02: The organization's hardware, software, and data assets are prioritized for protection based on their sensitivity, criticality, vulnerability, business value, and dependency role in the delivery of critical services.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #asset_classification_and_criticality | #asset_inventory | #asset_management | #business_impact_analysis | #dependency_management | #policy_management | #vulnerability_management

Response Guidance:

As referenced in ID.AM-05.01, the organization implements and maintains a policy on data classification. Classification enables the organization to determine the sensitivity, criticality, vulnerability, business value, and dependency role of resources and prioritize assets accordingly to their classification. The asset priority will guide management's decisions regarding internal controls, and processes and security standards, and help assess controls applied by contracted third parties.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Provide information on how critical assets are defined, classified, and prioritized (such as through a Business Impact Analysis). Describe the tools used to enable the organization to track, update, and provide custom reporting of the IT asset inventory (e.g., for vulnerability management, end-of-life/lifecycle management, business continuity plans, etc.).

Examples of Effective Evidence:

EEE-010: IT Asset Management and Business Function Mapping Documentation

- Inventory list of IT assets, including hardware, software, and data.
- Business function catalog that maps key assets to their corresponding business process.
- Asset ownership and stewardship records indicating who is responsible for specific assets.
- Lifecycle management records for assets, showing purchase dates, warranty periods, and disposal information.
- Integration diagrams showing how assets interact within the business's technology ecosystem.

EEE-034: Asset Management and Inventory Oversight Documentation

- Asset management policies that outline the processes and data requirements for tracking, maintaining, and securing organizational assets.
- Inventory lists or databases of assets, including hardware, software, data, and intellectual property, with assigned custodians or owners.
- Change logs or records of asset transfers, disposals, and acquisitions.
- Technical documentation and configuration of automated inventory discovery and management tools.
- Reports from periodic asset audits or reviews, confirming the accuracy of the inventory and compliance with the policy.
- Documentation of asset classification and labeling, indicating the criticality and sensitivity of assets.

EEE-045: Data Governance and Lifecycle Management Policy Documentation

- Data governance charters or policies that define the management of data throughout its lifecycle.
- Procedures and controls for data creation, storage, usage, archiving, and destruction.
- Documentation of data lifecycle workflows, including roles involved at each stage.
- Records of data quality assessments and data cleansing activities.
- Reports on compliance with legal and regulatory requirements related to data lifecycle management.

EEE-065: Asset Management and Custodianship Documentation

- Asset management policies that outline the procedures for asset custodianship, including accountability for asset security and maintenance.
- Records of asset assignments to custodians, including acknowledgment of responsibilities.
- Audit trails showing the tracking and verification of asset location, status, and custodianship.
- Reports from periodic reviews of asset management practices and custodian performance.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.
- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

IDENTIFY / Asset Management / Data & Metadata Inventory

ID.AM-07.01: The organization maintains a current inventory of the data being created, stored, or processed by its information assets and data flow diagrams depicting key internal and external data flows.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #asset_inventory | #asset_management | #business_impact_analysis | #dependency_management

Response Guidance:

A data inventory is a comprehensive record of an organization's data repositories (e.g., customer information files or storage area network) as needed for effective management. A current inventory is updated as frequently as necessary for the organization to successfully manage downstream processes reliant on an accurate data inventory. However, management should update the asset inventory and its classifications at least annually, or more frequently depending on risk, and should identify new data classifications. Data classification is the identification and organization of information according to its criticality and sensitivity and usage.

Describe the processes, tools, and data flow diagrams related to the inventory which includes types of data being created, stored, or processed by its information assets (e.g., cash positions, HR data, customer PII, trade data, post trade data, etc.). The organization should prioritize assets according to their classification in order to implement appropriate controls.

Examples of Effective Evidence:

EEE-010: IT Asset Management and Business Function Mapping Documentation

- Inventory list of IT assets, including hardware, software, and data.
- Business function catalog that maps key assets to their corresponding business process.
- Asset ownership and stewardship records indicating who is responsible for specific assets.
- Lifecycle management records for assets, showing purchase dates, warranty periods, and disposal information.
- Integration diagrams showing how assets interact within the business's technology ecosystem.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-011: External Dependencies and Risk Assessment Documents

- Diagrams of network architecture showing connections to external systems and services.
- Contracts and service level agreements (SLAs) with key vendors and service providers.
- Risk assessments of external dependencies highlighting potential impact on business operations.
- Documentation of alternative vendors and backup resources in case of primary vendor failure.
- Incident reports related to external dependencies, including response and resolution details.

EEE-045: Data Governance and Lifecycle Management Policy Documentation

- Data governance charters or policies that define the management of data throughout its lifecycle.
- Procedures and controls for data creation, storage, usage, archiving, and destruction.
- Documentation of data lifecycle workflows, including roles involved at each stage.
- Records of data quality assessments and data cleansing activities.
- Reports on compliance with legal and regulatory requirements related to data lifecycle management.

IDENTIFY / Asset Management / Asset Life Cycle Management

ID.AM-08.01: The organization establishes and maintains asset lifecycle management policies and procedures to ensure that assets are acquired, tracked, implemented, used, decommissioned, and protected commensurate with their sensitivity, criticality, and business value.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #asset_inventory | #asset_management | #critical_infrastructure | #data_classification | #data_lifecycle | #physical_infrastructure | #policy_management

Response Guidance:

An asset lifecycle is the sequence of stages that organizational assets go through during the time span of ownership. Provide information on how the organization implements cybersecurity and technology management considerations into their asset lifecycle management policies and procedures to formally manage assets from acquisition to end-of-life commensurate with their sensitivity, criticality, and business value.

The organization should prioritize assets according to their data classification in order to implement appropriate controls commensurate with their sensitivity, criticality, and business value. Describe the policies, procedures, processes and tools related to how the organization acquires, tracks, implements, uses, decommissions, and protects assets.

Examples of Effective Evidence:

EEE-010: IT Asset Management and Business Function Mapping Documentation

- Inventory list of IT assets, including hardware, software, and data.
- Business function catalog that maps key assets to their corresponding business process.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Asset ownership and stewardship records indicating who is responsible for specific assets.
- Lifecycle management records for assets, showing purchase dates, warranty periods, and disposal information.
- Integration diagrams showing how assets interact within the business's technology ecosystem.

EEE-034: Asset Management and Inventory Oversight Documentation

- Asset management policies that outline the processes and data requirements for tracking, maintaining, and securing organizational assets.
- Inventory lists or databases of assets, including hardware, software, data, and intellectual property, with assigned custodians or owners.
- Change logs or records of asset transfers, disposals, and acquisitions.
- Technical documentation and configuration of automated inventory discovery and management tools.
- Reports from periodic asset audits or reviews, confirming the accuracy of the inventory and compliance with the policy.
- Documentation of asset classification and labeling, indicating the criticality and sensitivity of assets.

EEE-065: Asset Management and Custodianship Documentation

- Asset management policies that outline the procedures for asset custodianship, including accountability for asset security and maintenance.
- Records of asset assignments to custodians, including acknowledgment of responsibilities.
- Audit trails showing the tracking and verification of asset location, status, and custodianship.
- Reports from periodic reviews of asset management practices and custodian performance.

ID.AM-08.02: The organization establishes policies, and employs methods to identify, assess, and manage technology solutions that are acquired, managed, or used outside of established, governed technology and cybersecurity processes (i.e., "Shadow IT").

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #asset_inventory | #asset_management | #policy_management

Response Guidance:

Describe how the organization identifies, assesses, and manages official (e.g., business unit) uses of technology solutions. Provide information on processes and tools used to detect, track, and analyze all systems that are acquired, managed, or used outside of internal established, governed technology and cybersecurity development and acquisition processes.

Organizations should employ processes and tools related to maintaining a complete asset inventory comprehensive of all assets. Include how accountability for data within the asset inventory is managed, how the inventory is updated through discovery of assets and maintain current information, as well as roles and responsibilities. Responses should include evidence of discovery tools, and continuous monitoring to identify “Shadow IT” that are connected to the organization’s network.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

Organizations should employ procurement policies and processes to disallow technology purchases that have not been appropriately reviewed and approved.

Examples of Effective Evidence:

EEE-010: IT Asset Management and Business Function Mapping Documentation

- Inventory list of IT assets, including hardware, software, and data.
- Business function catalog that maps key assets to their corresponding business process.
- Asset ownership and stewardship records indicating who is responsible for specific assets.
- Lifecycle management records for assets, showing purchase dates, warranty periods, and disposal information.
- Integration diagrams showing how assets interact within the business's technology ecosystem.

EEE-011: External Dependencies and Risk Assessment Documents

- Diagrams of network architecture showing connections to external systems and services.
- Contracts and service level agreements (SLAs) with key vendors and service providers.
- Risk assessments of external dependencies highlighting potential impact on business operations.
- Documentation of alternative vendors and backup resources in case of primary vendor failure.
- Incident reports related to external dependencies, including response and resolution details.

EEE-034: Asset Management and Inventory Oversight Documentation

- Asset management policies that outline the processes and data requirements for tracking, maintaining, and securing organizational assets.
- Inventory lists or databases of assets, including hardware, software, data, and intellectual property, with assigned custodians or owners.
- Change logs or records of asset transfers, disposals, and acquisitions.
- Technical documentation and configuration of automated inventory discovery and management tools.
- Reports from periodic asset audits or reviews, confirming the accuracy of the inventory and compliance with the policy.
- Documentation of asset classification and labeling, indicating the criticality and sensitivity of assets.

EEE-065: Asset Management and Custodianship Documentation

- Asset management policies that outline the procedures for asset custodianship, including accountability for asset security and maintenance.
- Records of asset assignments to custodians, including acknowledgment of responsibilities.
- Audit trails showing the tracking and verification of asset location, status, and custodianship.
- Reports from periodic reviews of asset management practices and custodian performance.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

IDENTIFY / Asset Management / Asset Life Cycle Management

ID.AM-08.03: The organization establishes policies, standards, and procedures for data governance, data management, and data retention consistent with its legal obligations and the value of data as an organizational asset.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #compliance | #data_protection | #data_retention | #policy_management

Response Guidance:

The organization should have data lifecycle policies, standards, and procedures in place to govern the classification inventory, and retention of data. Provide information on how these are evaluated, maintained, implemented, reviewed, and approved by the governing body. Provide information on how policies, standards, and procedures for data governance, data management, and data retention are defined consistent with legal obligations and the value of data as an organizational asset.

Describe how the organization defines roles and responsibilities that facilitate and effectively manage data management policies, standards, and procedures. Describe how data is classified, maintained, stored, retained, and destroyed according to the organization's data retention policy and how those data retention policies integrate applicable data retention laws and regulations.

Examples of Effective Evidence:

EEE-041: Data Governance and Retention Policy Documentation

- Data governance framework documents that outline roles, responsibilities, and processes for managing organizational data.
- Data retention schedules and policies specifying how long different types of data should be kept and the procedures for data disposal.
- Audit reports demonstrating compliance with data management and retention policies.
- Documentation of automated and manual processes used to implement data retention requirements.
- Training records for staff on data governance practices and data handling procedures.
- Documentation of data classification schemes used to manage data based on its sensitivity and importance.

EEE-045: Data Governance and Lifecycle Management Policy Documentation

- Data governance charters or policies that define the management of data throughout its lifecycle.
- Procedures and controls for data creation, storage, usage, archiving, and destruction.
- Documentation of data lifecycle workflows, including roles involved at each stage.
- Records of data quality assessments and data cleansing activities.
- Reports on compliance with legal and regulatory requirements related to data lifecycle management.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

ID.AM-08.04: The organization's asset management processes ensure the protection of sensitive data throughout removal, transfers, maintenance, end-of-life, and secure disposal or re-use.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #asset_management | #data_classification | #data_lifecycle | #data_protection

Response Guidance:

An asset lifecycle is the sequence of stages that organizational assets go through during the time span of ownership. The organization should monitor and analyze the risks associated with the organization's assets through termination or disposal, with particular attention to protecting sensitive data through the asset's lifecycle.

Provide information on the organization's asset management process. Describe how the assets are formally managed throughout removal, procurement, configuration, implementation into production, transfers, end-of-life, and secure disposal, or re-use of equipment processes, among other processes. Describe how data residing on the organization's assets is protected through the asset's lifecycle.

Examples of Effective Evidence:

EEE-034: Asset Management and Inventory Oversight Documentation

- Asset management policies that outline the processes and data requirements for tracking, maintaining, and securing organizational assets.
- Inventory lists or databases of assets, including hardware, software, data, and intellectual property, with assigned custodians or owners.
- Change logs or records of asset transfers, disposals, and acquisitions.
- Technical documentation and configuration of automated inventory discovery and management tools.
- Reports from periodic asset audits or reviews, confirming the accuracy of the inventory and compliance with the policy.
- Documentation of asset classification and labeling, indicating the criticality and sensitivity of assets.

EEE-045: Data Governance and Lifecycle Management Policy Documentation

- Data governance charters or policies that define the management of data throughout its lifecycle.
- Procedures and controls for data creation, storage, usage, archiving, and destruction.
- Documentation of data lifecycle workflows, including roles involved at each stage.
- Records of data quality assessments and data cleansing activities.
- Reports on compliance with legal and regulatory requirements related to data lifecycle management.

EEE-065: Asset Management and Custodianship Documentation

- Asset management policies that outline the procedures for asset custodianship, including accountability for asset security and maintenance.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of asset assignments to custodians, including acknowledgment of responsibilities.
- Audit trails showing the tracking and verification of asset location, status, and custodianship.
- Reports from periodic reviews of asset management practices and custodian performance.

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.
- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

ID.AM-08.05: The organization defines and implements standards and procedures, consistent with its data retention policy, for destroying or securely erasing data, media, and storage devices when the data is no longer needed.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #data_lifecycle | #data_protection | #data_retention | #policy_management

Response Guidance:

Provide information on the organization's data retention policy, standard, and framework. Provide information on the organizational structure as it pertains to data retention. Describe how data is maintained, stored, retained, and destroyed according to the organization's data retention policy and how those data retention policies integrate applicable data retention laws and regulations.

Examples of Effective Evidence:

EEE-041: Data Governance and Retention Policy Documentation

- Data governance framework documents that outline roles, responsibilities, and processes for managing organizational data.
- Data retention schedules and policies specifying how long different types of data should be kept and the procedures for data disposal.
- Audit reports demonstrating compliance with data management and retention policies.
- Documentation of automated and manual processes used to implement data retention requirements.
- Training records for staff on data governance practices and data handling procedures.
- Documentation of data classification schemes used to manage data based on its sensitivity and importance.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-045: Data Governance and Lifecycle Management Policy Documentation

- Data governance charters or policies that define the management of data throughout its lifecycle.
- Procedures and controls for data creation, storage, usage, archiving, and destruction.
- Documentation of data lifecycle workflows, including roles involved at each stage.
- Records of data quality assessments and data cleansing activities.
- Reports on compliance with legal and regulatory requirements related to data lifecycle management.

ID.AM-08.06: Minimum cybersecurity requirements for third-parties cover the entire relationship lifecycle, from the acquisition of data through the return or destruction of data, to include limitations on data use, access, storage, and geographic location.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authentication | #authorization | #data_lifecycle | #data_loss_prevention | #data_protection | #identity_and_access_management | #third_party_risk_management | #supply_chain_management

Response Guidance:

As referenced in EX.CN-02.01, the organization has documented minimum cybersecurity requirements for third parties. Describe how the minimum cybersecurity requirements for third parties cover the entire relationship lifecycle, including return or destruction of data, to include limitations on data use, access, storage, and geographic location. Management should consider including termination rights and recourse in contracts for a variety of conditions, including failure to meet cybersecurity requirements. Contracts should include provisions for timely return or destruction of the organization's data and resources. Include evidence from the third party documenting that data has been destroyed, such as an attestation or certification of destruction.

In outsourcing to cloud service providers, the potential that data are not completely removed or deleted from the servicer's storage media at the conclusion of a service contract may pose higher risk in a cloud computing environment than in traditional outsourcing. It is important to ensure that the cloud service provider can remove confidential data from all locations upon termination of the relationship.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

IDENTIFY / Risk Assessment / Asset Vulnerability Identification

ID.RA-01.01: The organization identifies, assesses, and documents risks and potential vulnerabilities associated with assets, to include workforce, data, technology, facilities, services, and connections.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #asset_management | #infrastructure_security | #insider_threat | #physical_security | #risk_management | #staffing_and_resource_management | #vulnerability_management

Response Guidance:

Provide information on how the organization, at the enterprise and business unit (or lines of business) level, identifies, assesses, and documents risks and potential vulnerabilities. Describe how the organization's (lines of business) assessments of technology and cyber risks and vulnerabilities link to, or are associated with assets, workforce, data, technology, facilities, services, and connections. Reference current risk management frameworks and processes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-010: IT Asset Management and Business Function Mapping Documentation

- Inventory list of IT assets, including hardware, software, and data.
- Business function catalog that maps key assets to their corresponding business process.
- Asset ownership and stewardship records indicating who is responsible for specific assets.
- Lifecycle management records for assets, showing purchase dates, warranty periods, and disposal information.
- Integration diagrams showing how assets interact within the business's technology ecosystem.

EEE-046: Risk Assessment and Threat Analysis Documentation

- Standardized risk assessment templates.
- Completed assessments for relevant organizational assets and processes.
- Threat analysis reports that identify potential threats and their likelihood and impact on the organization.
- Documentation of risk assessment training for staff involved in the risk management process.
- Risk registers or databases that track identified risks and their mitigation status.
- Historical trend analysis of threats and incidents to inform future risk assessments.

ID.RA-01.02: The organization's business units ensure that information regarding cyber risk is shared with the appropriate level of senior management in a timely manner, so that they can address and respond to emerging cyber risk.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #emerging_technologies | #risk_management | #threat_management

Response Guidance:

The organization’s Board or a Board committee and management will hold each business unit accountable for managing cyber risk.

Describe the process for how the lines of business ensure that information regarding cyber risk is shared with the appropriate level of senior management in a timely manner, and/or according to regulatory requirements, so that they can address and respond to emerging cyber risk. Provide information on related governance and risk frameworks, committees, and reporting.

Examples of Effective Evidence:

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.
- Risk management review reports that are presented to the board, including findings and recommendations.
- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.
- Training materials for board members on risk management principles and their oversight responsibilities.

ID.RA-01.03: The organization establishes and maintains standards and capabilities for ongoing vulnerability management, including systematic scans, or reviews reasonably designed to identify known cyber vulnerabilities and upgrade opportunities, across the organization's environments and assets.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #asset_management | #patch_management | #risk_management | #vulnerability_management

Response Guidance:

Describe how the organization has established and maintains standards and capabilities for ongoing vulnerability management, including systematic scans or reviews reasonably designed to identify known cyber vulnerabilities. Describe how the organization determines eligibility and coverage for vulnerability scanning. Provide information on the processes and tools utilized to conduct systematic scans or reviews. Provide information on the assessment process after performing vulnerability management.

Describe how the organization conducts ongoing vulnerability scanning, including automated scanning across the organization’s environments and assets, to identify potential system vulnerabilities including known vulnerabilities, and upgrade opportunities. Provide information of strategy and scope. Provide information regarding the tools utilized. Describe any comparisons or reconciliations with asset inventories to ensure that all intended assets and environments are scanned.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.
- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.
- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

IDENTIFY / Risk Assessment / Information Sharing Forums

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

ID.RA-02.01: The organization participates actively (in alignment with its business operations, inherent risk, and complexity) in information-sharing groups and collectives (e.g., cross-industry, cross-government and cross-border groups) to gather, distribute and analyze information about cyber practices, cyber threats, and early warning indicators relating to cyber threats.

Subject Tags: #emerging_technologies | #information_sharing | #mission_and_strategy | #risk_management | #security_logging_monitoring_and_alerting | #threat_management

Response Guidance:

Vulnerabilities and emerging threats are ever-changing and increasing. Situational awareness is considered foundational to effective cybersecurity risk management. As a result, organizations should participate in and subscribe to information sharing resources appropriate to its global operational footprint that include threat and vulnerability information for situational awareness. There are many sources of information, such as national CERTs, critical infrastructure sector information sharing and analysis centers (ISACs), industry associations, vendors, and government briefings. The organization should collaborate with law enforcement or information-sharing organizations in the jurisdictions where it does business to receive external threat and vulnerability information. Management should also establish a dedicated group to perform threat information analysis and develop and implement standard practices for evaluating threat information based on the source of the information and its relevance to the organization.

Provide details regarding the organization's engagements with cyber-related information-sharing groups.

Describe the linkage to the gathering, distribution, and analysis of information about cyber practices, cyber threats, and early warning indicators relating to cyber threats. Provide information related to the type of information received or shared and the level of engagement for each (e.g., notification-based, participation-based).

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-084: Cyber Threat Intelligence Sharing and Distribution Documents

- Policies and procedures for collecting, analyzing, and distributing cyber threat intelligence within the organization and with external partners.
- Agreements or memberships with threat intelligence sharing platforms or industry groups.
- Records of threat intelligence briefings or alerts issued to relevant stakeholders.
- Evaluations of the threat intelligence program, assessing its contribution to the organization's security posture.

EEE-101: Cyber Threat Intelligence Sharing Documentation

- Cyber threat intelligence policies that outline the process for collecting, analyzing, and sharing threat information.
- Records of threat intelligence received and shared with internal stakeholders and external partners.
- Analysis reports based on threat intelligence that inform security strategies and operations.
- Training records for security analysts on threat intelligence tools and analysis techniques.
- Membership or participation records in threat intelligence sharing platforms or industry groups.

ID.RA-02.02: The organization shares authorized information on its cyber resilience framework and the effectiveness of protection technologies bilaterally with trusted external stakeholders to promote the understanding of each party's approach to securing systems.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #disaster_recovery | #information_sharing | #resilience | #review_assessment_and_testing

Response Guidance:

The organization should have formal procedures in place to facilitate information sharing and should identify a network of trusted partners to securely communicate and evaluate cyber threats. The organization should also participate in and subscribe to information sharing resources that include threat and vulnerability information, such as with a national CERT, critical infrastructure information sharing and analysis centers (ISACs), industry associations, vendors, and government briefings. By sharing cyber threat and incident data with appropriate parties, the financial sector may benefit by enabling other organizations to assess and respond to current attacks.

A cyber resilience framework is an organization's ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources. Describe how the organization shares information on its cyber resilience framework bilaterally with trusted external stakeholders to promote understanding of each other's approach to securing systems that are linked or interfaced.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Describe how the organization shares appropriate types of information about the effectiveness of its protection technologies with appropriate parties. Describe the roles and responsibilities of the team who performs the information sharing, the types of information that is shared, what organizations are shared with, and the process of sharing information.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-060: Cross-Sector Incident Response Coordination Documents

- Coordination plans that outline how the organization will work with external entities during an incident response.
- Agreements or MOUs with cross-sector partners and government agencies for collaborative information sharing and/orincident response.
- After-action reports from joint incident response exercises with cross-sector partners.
- Communication protocols for sharing information and coordinating actions during cross-sector incidents.
- Training and exercise records for staff on cross-sector incident response procedures.

EEE-084: Cyber Threat Intelligence Sharing and Distribution Documents

- Policies and procedures for collecting, analyzing, and distributing cyber threat intelligence within the organization and with external partners.
- Agreements or memberships with threat intelligence sharing platforms or industry groups.
- Records of threat intelligence briefings or alerts issued to relevant stakeholders.
- Evaluations of the threat intelligence program, assessing its contribution to the organization's security posture.

EEE-101: Cyber Threat Intelligence Sharing Documentation

- Cyber threat intelligence policies that outline the process for collecting, analyzing, and sharing threat information.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of threat intelligence received and shared with internal stakeholders and external partners.
- Analysis reports based on threat intelligence that inform security strategies and operations.
- Training records for security analysts on threat intelligence tools and analysis techniques.
- Membership or participation records in threat intelligence sharing platforms or industry groups.

IDENTIFY / Risk Assessment / Threat Identification

ID.RA-03.01: The organization, on an ongoing basis, identifies, analyzes, correlates, characterizes, and reports threats that are internal and external to the firm.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #threat_landscape | #threat_management

Response Guidance:

The organization conducts a cyber threat analysis, on an ongoing basis, to identify cyber threats from internal and external sources that could materially affect its ability to perform or to provide services as expected. Threat intelligence gathering involves the acquisition and analysis of this information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance the organization's decision-making. The organization should establish an ongoing process to gather, analyze, correlate, characterize, and report relevant cyber threat information, including threats reported by third parties. Practices should be established for information sharing and reporting threats with third parties to understand both internal and external threats relevant to the firm.

Describe the framework and processes used within the organization to identify, document, and analyze internal and external threats to the organization. Provide information regarding the threat intelligence structure and process.

Examples of Effective Evidence:

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-084: Cyber Threat Intelligence Sharing and Distribution Documents

- Policies and procedures for collecting, analyzing, and distributing cyber threat intelligence within the organization and with external partners.
- Agreements or memberships with threat intelligence sharing platforms or industry groups.
- Records of threat intelligence briefings or alerts issued to relevant stakeholders.
- Evaluations of the threat intelligence program, assessing its contribution to the organization's security posture.

EEE-101: Cyber Threat Intelligence Sharing Documentation

- Cyber threat intelligence policies that outline the process for collecting, analyzing, and sharing threat information.
- Records of threat intelligence received and shared with internal stakeholders and external partners.
- Analysis reports based on threat intelligence that inform security strategies and operations.
- Training records for security analysts on threat intelligence tools and analysis techniques.
- Membership or participation records in threat intelligence sharing platforms or industry groups.

ID.RA-03.02: The organization solicits and considers threat intelligence received from the organization's stakeholders, service and utility providers, and other industry and security organizations.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #threat_landscape | #threat_management

Response Guidance:

Vulnerabilities and emerging threats are ever changing and increasing. Situational awareness is considered foundational to effective cybersecurity risk management. As a result, organizations should subscribe to information sharing resources that include threat and vulnerability information for situational awareness.

Proactively sharing threat intelligence helps organizations achieve broader cybersecurity situational awareness among external stakeholders. Once validated, the organization’s threat intelligence should be shared as appropriate.

Describe how input from the organization’s stakeholders, service and utility providers, and other industry and security organizations are reviewed, analyzed, aggregated, and considered as part of threat intelligence. Describe how customers, partners, researchers, or other external parties can report threats or suspected vulnerabilities to the organization.

Examples of Effective Evidence:

EEE-084: Cyber Threat Intelligence Sharing and Distribution Documents

- Policies and procedures for collecting, analyzing, and distributing cyber threat intelligence within the organization and with external partners.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

- Agreements or memberships with threat intelligence sharing platforms or industry groups.
- Records of threat intelligence briefings or alerts issued to relevant stakeholders.
- Evaluations of the threat intelligence program, assessing its contribution to the organization's security posture.

EEE-101: Cyber Threat Intelligence Sharing Documentation

- Cyber threat intelligence policies that outline the process for collecting, analyzing, and sharing threat information.
- Records of threat intelligence received and shared with internal stakeholders and external partners.
- Analysis reports based on threat intelligence that inform security strategies and operations.
- Training records for security analysts on threat intelligence tools and analysis techniques.
- Membership or participation records in threat intelligence sharing platforms or industry groups.

ID.RA-03.03: The organization includes in its threat analysis those cyber threats which could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred in the past.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #threat_landscape | #threat_management

Response Guidance:

Threat information is correlated to an organization’s vulnerabilities and other factors to provide the organization with a risk calculation. Threat information should integrate with intrusion prevention, intrusion detection, and data loss prevention technologies to provide alerts and real-time remediation of threat activity. Organizations should utilize tabletop exercises as an effective way to identify potential threats and vulnerabilities not readily identified by other means.

Provide information on the analysis of cyber threats that could trigger extreme but plausible events regardless of likelihood. Describe how the analysis considers cyber threats across all event likelihoods.

Examples of Effective Evidence:

EEE-046: Risk Assessment and Threat Analysis Documentation

- Standardized risk assessment templates.
- Completed assessments for relevant organizational assets and processes.
- Threat analysis reports that identify potential threats and their likelihood and impact on the organization.
- Documentation of risk assessment training for staff involved in the risk management process.
- Risk registers or databases that track identified risks and their mitigation status.
- Historical trend analysis of threats and incidents to inform future risk assessments.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

ID.RA-03.04: The organization regularly reviews and updates its threat analysis methodology, threat information sources, and supporting tools.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #threat_landscape | #threat_management

Response Guidance:

As referenced in ID.RA-03.01, the organization conducts a cyber threat analysis to identify cyber threats that could materially affect its ability to perform or to provide services as expected. The organization should regularly review and update its threat analysis methodology, threat information sources, and supporting tools. Response should provide information on how the organization performs threat information analysis and develops and implements methodologies and standard practices for evaluating threat information based on the source of the information and its relevance to the organization.

Provide information on how the organization regularly reviews and updates the results of its cyber threat analysis methodology, threat information sources, and supporting tools. Provide information on how the organization reviews the organization's engagements with cyber-related information-sharing groups to reflect an organization participating and subscribing to information sharing resources appropriate to its global operational footprint.

Examples of Effective Evidence:

EEE-046: Risk Assessment and Threat Analysis Documentation

- Standardized risk assessment templates.
- Completed assessments for relevant organizational assets and processes.
- Threat analysis reports that identify potential threats and their likelihood and impact on the organization.
- Documentation of risk assessment training for staff involved in the risk management process.
- Risk registers or databases that track identified risks and their mitigation status.
- Historical trend analysis of threats and incidents to inform future risk assessments.

EEE-084: Cyber Threat Intelligence Sharing and Distribution Documents

- Policies and procedures for collecting, analyzing, and distributing cyber threat intelligence within the organization and with external partners.
- Agreements or memberships with threat intelligence sharing platforms or industry groups.
- Records of threat intelligence briefings or alerts issued to relevant stakeholders.
- Evaluations of the threat intelligence program, assessing its contribution to the organization's security posture.

EEE-101: Cyber Threat Intelligence Sharing Documentation

- Cyber threat intelligence policies that outline the process for collecting, analyzing, and sharing threat information.
- Records of threat intelligence received and shared with internal stakeholders and external partners.
- Analysis reports based on threat intelligence that inform security strategies and operations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Training records for security analysts on threat intelligence tools and analysis techniques.
- Membership or participation records in threat intelligence sharing platforms or industry groups.

IDENTIFY / Risk Assessment / Impact & Likelihood Analysis

ID.RA-04.01: The organization's risk assessment approach includes the analysis and characterization of the likelihood and potential business impact of identified risks being realized.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #business_impact_analysis | #review_assessment_and_testing | #risk_management | #threat_management

Response Guidance:

Cyber risks can lead to financial, strategic, regulatory, and compliance impacts. For example, a data breach can result in customer notification and credit monitoring costs, as well as reputational damage and regulatory fines. The organization should track the financial impact cyber incidents may have on the organization's capital.

Analyzing the financial impact associated with cybersecurity incidents helps an organization align and prioritize resources to risks with greater financial impacts.

Provide information on how the risk assessment approach includes the identification of the likelihood and potential business impact of cyber risks.

Examples of Effective Evidence:

EEE-046: Risk Assessment and Threat Analysis Documentation

- Standardized risk assessment templates.
- Completed assessments for relevant organizational assets and processes.
- Threat analysis reports that identify potential threats and their likelihood and impact on the organization.
- Documentation of risk assessment training for staff involved in the risk management process.
- Risk registers or databases that track identified risks and their mitigation status.
- Historical trend analysis of threats and incidents to inform future risk assessments.

IDENTIFY / Risk Assessment / Risk Exposure Determination & Prioritization

ID.RA-05.01: Threats, vulnerabilities, likelihoods, and impacts are used to determine overall technology, cybersecurity, and resilience risk to the organization.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #incident_management | #resilience | #risk_management | #threat_management

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

The organization's risk assessment methodology should include the analysis of threats, vulnerabilities, likelihoods, and impacts in the determination and characterization of risks to the organization. Threat intelligence gathering and assessment involves the acquisition and analysis of this information to identify, track, and predict cyber capabilities, intentions, and activities of malicious actors and can inform the overall technology, cybersecurity, and resilience risk to the organization. Integration and analysis of threat intelligence should inform the organization's decision-making regarding technology, cybersecurity, and resilience risk reduction activities.

Provide information showing threat, vulnerability, likelihood, and impact assessments are linked to the overall evaluation of technology, cybersecurity, and resilience risk to the organization.

Examples of Effective Evidence:

EEE-046: Risk Assessment and Threat Analysis Documentation

- Standardized risk assessment templates.
- Completed assessments for relevant organizational assets and processes.
- Threat analysis reports that identify potential threats and their likelihood and impact on the organization.
- Documentation of risk assessment training for staff involved in the risk management process.
- Risk registers or databases that track identified risks and their mitigation status.
- Historical trend analysis of threats and incidents to inform future risk assessments.

ID.RA-05.02: The organization has established threat modeling capabilities to identify how and why critical assets might be compromised by a threat actor, what level of protection is needed for those critical assets, and what the impact would be if that protection failed.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #critical_infrastructure | #threat_landscape | #threat_management

Response Guidance:

Threat modeling is a structured approach that enables an organization to aggregate and quantify the impact of potential threats.

Describe what threat modeling capabilities the organization has established. Provide information regarding the established threat modeling capabilities that support the identification of how and why critical assets might be compromised by a threat actor, what level of protection is needed, and what the impact would be if the protection failed.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-046: Risk Assessment and Threat Analysis Documentation

- Standardized risk assessment templates.
- Completed assessments for relevant organizational assets and processes.
- Threat analysis reports that identify potential threats and their likelihood and impact on the organization.
- Documentation of risk assessment training for staff involved in the risk management process.
- Risk registers or databases that track identified risks and their mitigation status.
- Historical trend analysis of threats and incidents to inform future risk assessments.

ID.RA-05.03: The organization's business units assess, on an ongoing basis, the technology, cybersecurity, and resilience risks associated with the activities of the business unit.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #resilience | #review_assessment_and_testing | #risk_management

Response Guidance:

Technology, cybersecurity, and resilience risks are always evolving and can lead to financial, strategic, regulatory, and compliance impacts.

Provide information regarding how the organization's business units continually assess technology, cybersecurity, and resilience risk (e.g., risk governance framework, control assessments, etc.) and any models or frameworks used for the assessment. Describe how the risks are reported to senior management and/or enterprise risk management.

Examples of Effective Evidence:

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

ID.RA-05.04: The organization uses scenario planning, table-top-exercises, or similar event analysis techniques to identify vulnerabilities and determine potential impacts to critical infrastructure, technology, and business processes.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #business_impact_analysis | #critical_infrastructure | #disaster_recovery | #incident_management | #resilience | #scenario_risk_assessment | #vulnerability_management

Response Guidance:

Describe how the organization uses scenario planning, table-top-exercises, or similar event analysis techniques to identify vulnerabilities and determine potential impacts to critical infrastructure, technology, and business processes. For example, scenarios may include cyber events demonstrating the ability of the organization, as well as its third-party providers, to respond quickly and efficiently to a cyber incident, such as a DDoS attack. Tabletop exercises may also identify critical single points of failure in staff or other resources. Provide information on how organizations address potential single points of failure.

Examples of Effective Evidence:

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.
- Business continuity plan outlining procedures for maintaining service delivery during disruptions.
- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.
- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.
- Contingency plans detailing alternative service delivery methods.
- Training records for staff on resilience and continuity procedures and their roles during incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

IDENTIFY / Risk Assessment / Risk Response Determination

ID.RA-06.01: Technology and cybersecurity risk management programs and risk assessment processes produce actionable recommendations that the organization uses to select, design, prioritize, implement, maintain, evaluate, and modify cybersecurity and technology controls.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #enterprise_risk_management | #metrics_and_reporting | #program_transformation | #review_assessment_and_testing | #risk_management | #risk_response | #improvements

Response Guidance:

Management should have a methodology to measure and document technology and cybersecurity risks and for determining resources required for mitigating gaps. The technology and cybersecurity risk assessment should identify internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or other sensitive data and technology availability and business-it risks. Risk assessments should assess the likelihood and potential damage of these threats, and validate whether policies, procedures, and controls in place are appropriately mitigating risks. Organizations should produce and evaluate actionable recommendations to address risks identified from risk assessments. Results from the risk assessment should be formally presented to senior management and the Board (or other appropriate governing authority) at least annually.

Provide information related to the source of various risk assessments (internal/external) that produce actionable technology and cybersecurity recommendations that are prioritized and tracked. Provide evidence of technology and cybersecurity recommendations through the process of remediation.

Examples of Effective Evidence:

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-046: Risk Assessment and Threat Analysis Documentation

- Standardized risk assessment templates.
- Completed assessments for relevant organizational assets and processes.
- Threat analysis reports that identify potential threats and their likelihood and impact on the organization.
- Documentation of risk assessment training for staff involved in the risk management process.
- Risk registers or databases that track identified risks and their mitigation status.
- Historical trend analysis of threats and incidents to inform future risk assessments.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.
- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.
- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

ID.RA-06.02: The implementation of responses to address identified risks (i.e., risk avoidance, risk mitigation, risk acceptance, or risk transfer (e.g., cyber insurance)) are formulated, assessed, documented, and prioritized based on criticality to the business.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #enterprise_risk_management | #issue_management | #metrics_and_reporting | #risk_management | #risk_response

Response Guidance:

Responses should provide various methods for risk response, including risk avoidance, risk mitigation, risk acceptance, or risk transfer, based on the potential impact to the delivery of critical services and criticality to the business. The organization documents, assesses, formulates, and prioritizes identified risks to determine the appropriate response approach. Organizations use their risk management framework and processes to prioritize the implementation of responses.

Describe the processes and tools used to address identified cyber risks. Include information on the processes used for risk acceptance, risk mitigation, risk avoidance, or risk transfer, which includes cyber insurance. Provide examples supporting how a risk is mitigated (e.g., implementing new controls), justification if a risk is accepted, etc. Describe the role of various stakeholders in the formulation and prioritization of risk responses.

Examples of Effective Evidence:

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-005: Risk Appetite Tolerance, and Strategy Alignment Documents

- Risk appetite statements approved by the board or executive management.
- Risk tolerance levels defined for different categories of risk.
- Documentation on how risk appetite influences decision-making and strategy.
- Reports on risk exposures compared to the defined risk appetite.
- Updates or revisions to risk appetite and tolerance based on changing conditions.

ID.RA-06.03: Technology and cybersecurity programs identify and implement controls to manage applicable risks within the risk appetite set by the governing authority (e.g., the Board or one of its committees).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #enterprise_risk_management | #issue_management | #program_transformation | #risk_appetite_/_tolerance | #risk_management | #risk_oversight

Response Guidance:

The organization's management should have a process in place to identify all potential risks relevant to the organization, as well as a process to implement controls to manage applicable risks. Applicable risks should be managed according to the risk appetite set by the governing authority (e.g., the Board or one of its committees). Provide information on stakeholder involvement for control selection and design to manage applicable risks. Determine how new controls are integrated into technology and cybersecurity programs, as well as into technology and cybersecurity architecture, and assessed for ongoing effectiveness. Describe the organization's process to review the cost and control assessments in place for proposed controls. Policies, processes, and procedures should be in place to address decommissioning of old controls.

Examples of Effective Evidence:

EEE-004: Risk Management Framework and Reporting Documents

- Enterprise risk management (ERM) framework documentation.
- IT risk assessment reports identifying potential threats, vulnerabilities, controls, impacts, and mitigation recommendations.
- Risk register tracking identified risks and mitigation strategies.
- Annual risk management reports summarizing risk posture.
- Risk treatment plans detailing responses to specific risks.

EEE-005: Risk Appetite Tolerance, and Strategy Alignment Documents

- Risk appetite statements approved by the board or executive management.
- Risk tolerance levels defined for different categories of risk.
- Documentation on how risk appetite influences decision-making and strategy.
- Reports on risk exposures compared to the defined risk appetite.
- Updates or revisions to risk appetite and tolerance based on changing conditions.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

ID.RA-06.04: The organization assesses the threats, impacts, and risks that could adversely affect the organization's ability to provide services on an ongoing basis, and develops its resilience requirements and plans to address those risks.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #mission_and_strategy | #resilience | #risk_management | #threat_management

Response Guidance:

The organization conducts threat analysis to identify threats from internal and external sources that could materially affect its ability to perform or to provide services as expected. Describe the organization's engagement with information-sharing groups to gather, analyze, and assess applicable threats, impacts, and risks. Provide information on the analysis of cyber threats that could trigger extreme but plausible events regardless of likelihood (e.g., tabletop exercises). Provide information on how the risk assessment approach includes the identification of the likelihood and potential business impact of threats and risks that could adversely affect the organization's ability to provide services.

A resilience framework is an organization's ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include resources. Responses include resilience frameworks, plans, processes, and procedures in place to address threats, impacts, and risks that could adversely affect the organization's ability to provide services. Describe how the organization defines objectives for resumption of critical operations (recovery time objectives, recovery point objectives). Include information on the organization's business impact analysis, the scope of critical business processes, service dependencies, technology dependencies, and prioritization for recovery, among other details.

Examples of Effective Evidence:

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.
- Business continuity plan outlining procedures for maintaining service delivery during disruptions.
- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.
- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.
- Contingency plans detailing alternative service delivery methods.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Training records for staff on resilience and continuity procedures and their roles during incidents.

ID.RA-06.05: The organization defines and implements standards and procedures to prioritize and remediate issues identified in vulnerability scanning or penetration testing, including emergency or zero-day threats and vulnerabilities.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #issue_management | #patch_management | #penetration_testing | #policy_management | #threat_management | #vulnerability_management

Response Guidance:

Vulnerability management is a key control to ensure known vulnerabilities in systems, applications, and devices are uncovered before they are placed into production. Vulnerability scanning and/or penetration testing is normally conducted on a routine basis, as well as during systems development lifecycle, and acquisition activities.

Provide information on metrics and reporting used to prioritize and remediate issues identified. Describe what standards, procedures, and processes the organization has established to prioritize and remedy issues identified through vulnerability scanning and penetration testing. Issues identified should integrate patching processes, standards, and procedures in place. Describe the prioritization methodology, such as potential impact, time to remedy, etc., and the process for vulnerability scanning and penetration testing. Provide information of any exception procedures employed.

Examples of Effective Evidence:

EEE-036: Vulnerability Scanning and Patch Management Documentation

- Policy, standard, and/or procedure documents covering the identification, assessment, reporting, and remediation of software and device vulnerabilities, including regular patching protocols.
- Schedules and records of patch deployment activities, including system reboots, post-patch testing, dates, systems affected, and patching outcomes.
- Documentation of patching or upgrades to standard system configuration baselines.
- Reports from vulnerability scans or assessments that inform the patch management process.
- Incident reports related to vulnerabilities that were mitigated through patch management.
- Documentation and reporting of vulnerability mitigation targets.
- Records of exceptions to, assessments of, and approvals for cases where vulnerability mitigation targets or standards are not met.
- Records demonstrating the integration of patch management and change management practices.
- Approval and review documentation for patching protocols, including impact assessments and authorization records.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Dashboards or tools used to monitor patch levels and patch application across the target environment.
- Post-implementation reviews and post-change evaluation reports assessing the impact and success of patches and any unintended consequences.
- Audit or review findings related to vulnerability management and patching practices with actions taken in response to findings.

EEE-037: Change Management Documentation

- Policy, standard, and/or procedure documents covering change management practices.
- Change management procedures that outline the process for assessing, tracking, making and documenting changes to IT systems and business processes.
- Change management procedures for emergency changes, to include approval requirements and post-change documentation requirements.
- Change management records and documentation for system changes, reflecting updates, modifications, and controlled implementation.
- Change control records documenting the approval and implementation of system changes, patches, and configuration control, to include actions and decisions taken by change advisory boards or similar review groups.
- Approval and review documentation for changes, including impact assessments and authorization records.
- Post-implementation reviews and post-change evaluation reports assessing the impact and success of system changes, identifying any unintended consequences.
- Records demonstrating that change management practices are integrated into project delivery processes.
- Records demonstrating that documentation, training, and other system artifacts are updated to reflect any changes made.
- Audit or review findings related to change management, with actions taken in response to findings.

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.
- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.
- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

ID.RA-06.06: The organization follows documented procedures, consistent with established risk response processes, for mitigating or accepting the risk of vulnerabilities or weaknesses identified in exercises and testing or when responding to incidents.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #application_security | #application_security_testing | #enterprise_risk_management | #issue_management | #penetration_testing | #policy_management | #vulnerability_management

Response Guidance:

The organization should have procedures in place to restore system functionality after identifying vulnerabilities or weaknesses identified in exercises, testing or incident response. Describe how the organization's documented procedures are consistent with established risk response processes, for the mitigation or acceptance of any identified vulnerabilities or weaknesses identified in exercises and testing or when responding to incidents. Include information regarding the related steps in the incident management plan and post incident reviews.

Describe how any identified vulnerabilities or weaknesses identified as a result of exercises, testing, or incident response are mitigated or documented by the organization as accepted risks and monitored. Provide information on how the organization's formal exception or issue management process is part of this process for vulnerabilities that cannot be mitigated due to business-related exceptions.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.
- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

IDENTIFY / Risk Assessment / Change & Exception Management

ID.RA-07.01: The organization defines and implements change management standards and procedures, to include emergency change procedures, that explicitly address risk identified both prior to and during a change, any new risk created post-change, as well as the reviewing and approving authorities (e.g., change advisory boards).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #change_management | #policy_management | #risk_management | #risk_oversight

Response Guidance:

Change management involves a policy, procedures, and standards that guide a broad range of changes within an organization's operating environment. Changes may include configuration changes, such as security settings, hardware changes that address obsolescence, routine software releases, including those provided by a third party, or emergency fixes and patches that eliminate software or other vulnerabilities. Technology projects and system implementations may also introduce a broad range of changes, both technical and business-related, which should be managed effectively. To ensure risks and vulnerabilities are not introduced with changes, the change management process needs to include a security impact, business impact, or similar analysis.

Describe how the organization's change management process explicitly considers risks, in terms of residual risks identified both prior to and during a change, and of any new risk created post-change. Describe how pre- and post-change testing, and back-out plans, are integrated into the procedures. Describe how emergency changes may be handled differently than routine or standard changes. Provide information related to the change management process, and approval authorities (e.g., change advisory boards).

Examples of Effective Evidence:

EEE-037: Change Management Documentation

- Policy, standard, and/or procedure documents covering change management practices.
- Change management procedures that outline the process for assessing, tracking, making and documenting changes to IT systems and business processes.
- Change management procedures for emergency changes, to include approval requirements and post-change documentation requirements.
- Change management records and documentation for system changes, reflecting updates, modifications, and controlled implementation.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Change control records documenting the approval and implementation of system changes, patches, and configuration control, to include actions and decisions taken by change advisory boards or similar review groups.
- Approval and review documentation for changes, including impact assessments and authorization records.
- Post-implementation reviews and post-change evaluation reports assessing the impact and success of system changes, identifying any unintended consequences.
- Records demonstrating that change management practices are integrated into project delivery processes.
- Records demonstrating that documentation, training, and other system artifacts are updated to reflect any changes made.
- Audit or review findings related to change management, with actions taken in response to findings.

ID.RA-07.02: Risk-based criteria are used to categorize each system change, to include emergency changes, to determine the necessary change process standards to apply for change planning, rollback planning, pre-change testing, change access control, post-change verification, and change review and approval.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #change_management | #policy_management | #review_assessment_and_testing | #risk_management

Response Guidance:

Emergency changes are unscheduled changes needed to be implemented with high urgency due to the nature of the change (e.g., emergency fixes and patches that eliminate software or other vulnerabilities). Risk-based criteria should be defined and documented to categorize and prioritize each system change. Organizations should have standards, procedures, processes, and approvals for necessary changes and should be tested and validated prior to release and verified post-change. Describe the risks related to not making the proposed change, and how the organization implements rollback planning.

Provide information on how an organization determines risk-based criteria to prioritize each system change, including emergency changes. Processes should be in place for managing configuration changes to systems to include change advisory boards that review and approve change requests for change planning, rollback planning, pre-change testing, change access control, and post-control verification.

Examples of Effective Evidence:

EEE-037: Change Management Documentation

- Policy, standard, and/or procedure documents covering change management practices.
- Change management procedures that outline the process for assessing, tracking, making and documenting changes to IT systems and business processes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Change management procedures for emergency changes, to include approval requirements and post-change documentation requirements.
- Change management records and documentation for system changes, reflecting updates, modifications, and controlled implementation.
- Change control records documenting the approval and implementation of system changes, patches, and configuration control, to include actions and decisions taken by change advisory boards or similar review groups.
- Approval and review documentation for changes, including impact assessments and authorization records.
- Post-implementation reviews and post-change evaluation reports assessing the impact and success of system changes, identifying any unintended consequences.
- Records demonstrating that change management practices are integrated into project delivery processes.
- Records demonstrating that documentation, training, and other system artifacts are updated to reflect any changes made.
- Audit or review findings related to change management, with actions taken in response to findings.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

ID.RA-07.03: Technology projects and system change processes ensure that requisite changes in security posture, data classification and flows, architecture, support documentation, business processes, and business resilience plans are addressed.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #architecture | #change_management | #data_protection | #policy_management | #resilience | #risk_management | #risk_oversight

Response Guidance:

Changes in an organization's security posture, data classification and flows, architecture, support documentation, business processes, and business resilience plans should be aligned to technology projects and system change processes.

Provide information of established change management policies, procedures, and standards guide a broad range of changes within an organization's operating environment and consider updates to reflect the current business processes. Processes are in place for change requests, review, testing,

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

and approval of proposed changes to change advisory boards. Describe how business stakeholders may be engaged in broad changes resulting from project on a new system implementation.

Examples of Effective Evidence:

EEE-037: Change Management Documentation

- Policy, standard, and/or procedure documents covering change management practices.
- Change management procedures that outline the process for assessing, tracking, making and documenting changes to IT systems and business processes.
- Change management procedures for emergency changes, to include approval requirements and post-change documentation requirements.
- Change management records and documentation for system changes, reflecting updates, modifications, and controlled implementation.
- Change control records documenting the approval and implementation of system changes, patches, and configuration control, to include actions and decisions taken by change advisory boards or similar review groups.
- Approval and review documentation for changes, including impact assessments and authorization records.
- Post-implementation reviews and post-change evaluation reports assessing the impact and success of system changes, identifying any unintended consequences.
- Records demonstrating that change management practices are integrated into project delivery processes.
- Records demonstrating that documentation, training, and other system artifacts are updated to reflect any changes made.
- Audit or review findings related to change management, with actions taken in response to findings.

EEE-053: Project Governance, Management, and Quality Assurance Documentation

- Project governance frameworks or charters that define roles, responsibilities, and decision-making processes.
- Stakeholder analysis documents and communication plans for engaging with project stakeholders.
- Project management plans that include quality control measures, checkpoints, risk mitigation strategies, and contingency planning.
- Risk assessment templates and completed assessments for technology projects, identifying potential delivery risks.
- Quality assurance policies and procedures for overseeing project deliverables and outcomes.
- Checklists and tools used for quality control during project execution.
- Meeting minutes and action items from project steering committees, governance boards, or risk management discussions within project teams, including actions taken to address identified risks.
- Records of project audits or reviews focused on quality aspects.
- Feedback and satisfaction surveys from stakeholders regarding project outcomes and engagement.
- Reports on project performance, governance effectiveness, and risk management effectiveness, including lessons learned.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Training documentation for project managers and team members on quality management practices and risk assessment and management techniques.
- Post-project reviews or retrospectives that analyze risk management effectiveness and lessons learned.
- Documentation of project management standards, methodologies, and best practices adopted by the organization

ID.RA-07.04: Policy exceptions, risk mitigation plans, and risk acceptances resulting from assessments and evaluations, such as testing, exercises, audits, etc., are formally managed, approved, escalated to defined levels of management, and tracked to closure.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #enterprise_risk_management | #issue_management | #policy_management | #review_assessment_and_testing | #risk_management

Response Guidance:

Responses should provide risk management strategies, procedures, standards, and policies that are inclusive of policy exceptions, risk mitigation plans, and risk acceptances. Describe tracking of status on risks identified from testing, exercises, audits, etc. and the number/types of reports, including any dashboard which provide details on risks and threats identified, mitigating actions proposed and their status tracked until closure.

Provide information on the organization's formal exception management process for risks that cannot be mitigated. Describe the process of escalation of policy exceptions to defined levels of management, review/ongoing monitoring, and approval. Responses should provide evidence on an approved risk response prior to formal closure of any assessment and evaluation issue identified. Where risks may be accepted, identify any standards for re-review of the exception at regular intervals.

Examples of Effective Evidence:

EEE-048: Exception Management and Vulnerability Handling Documentation

- Policies and procedures for handling exceptions to standard security policies, including the process for requesting and approving exceptions.
- Documentation of approved policy exceptions, including justification, risk assessment, and compensating controls.
- Vulnerability exception records that detail the rationale for not remediating certain vulnerabilities and the associated risk acceptance.
- Audit reports that review the management of policy and vulnerability exceptions.

EEE-066: Segregation of Duties in Risk Management Documentation

- Policies and procedures that establish segregation of duties within risk management activities to prevent conflicts of interest and fraud.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Flowcharts or diagrams that illustrate the separation of roles and responsibilities in risk-related processes.
- Internal control reports that verify the effectiveness of segregation of duties in mitigating risks.
- Records of changes to duties or responsibilities to maintain proper segregation as the organization evolves.

ID.RA-07.05: The organization establishes and maintains an exception management process for identified vulnerabilities that cannot be mitigated within target timeframes.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #application_security | #application_security_testing | #issue_management | #penetration_testing | #policy_management | #review_assessment_and_testing | #risk_management | #vulnerability_management

Response Guidance:

Exception management processes should specifically address vulnerabilities that cannot be mitigated due to unsupported or end-of-life hardware, software, or applications. Provide information on the organization's exception management process for vulnerabilities that cannot be mitigated due to business-related exceptions. Describe the process of review and approval and ongoing monitoring/reporting of exceptions.

Examples of Effective Evidence:

EEE-048: Exception Management and Vulnerability Handling Documentation

- Policies and procedures for handling exceptions to standard security policies, including the process for requesting and approving exceptions.
- Documentation of approved policy exceptions, including justification, risk assessment, and compensating controls.
- Vulnerability exception records that detail the rationale for not remediating certain vulnerabilities and the associated risk acceptance.
- Audit reports that review the management of policy and vulnerability exceptions.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

IDENTIFY / Risk Assessment / Vulnerability Disclosure Response

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

ID.RA-08.01: The organization has established enterprise processes for soliciting, receiving and appropriately channeling vulnerability disclosures from:

(1) Public sources (e.g., customers and security researchers);

(2) Vulnerability sharing forums (e.g., FS-ISAC); and

(3) Third-parties (e.g., cloud vendors);

(4) Internal sources (e.g., development teams).

Subject Tags: #information_sharing | #issue_management | #third_party_risk_management | #threat_management | #vulnerability_management | #supply_chain_management

Response Guidance:

Describe the process for receiving and channeling vulnerability disclosures. Highlight the process related to each of the four sources in the statement (public, vulnerability sharing forums, third parties, and internal sources). Expectations for third-party vulnerability disclosure may be included in contracts and information sharing agreements.

Examples of Effective Evidence:

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-049: Vulnerability Disclosure and Response Protocol Documentation

- Procedures for receiving, assessing, and responding to vulnerability disclosures from external researchers, customers, or other entities.
- Communication templates and protocols for interacting with individuals or organizations reporting vulnerabilities.
- Records of disclosed vulnerabilities, including the organization's response and remediation actions.
- Agreements or MOUs with bug bounty platforms or security researchers regarding vulnerability disclosure.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Reports summarizing the outcomes of vulnerability disclosures and the effectiveness of the response process.

EEE-084: Cyber Threat Intelligence Sharing and Distribution Documents

- Policies and procedures for collecting, analyzing, and distributing cyber threat intelligence within the organization and with external partners.
- Agreements or memberships with threat intelligence sharing platforms or industry groups.
- Records of threat intelligence briefings or alerts issued to relevant stakeholders.
- Evaluations of the threat intelligence program, assessing its contribution to the organization's security posture.

EEE-101: Cyber Threat Intelligence Sharing Documentation

- Cyber threat intelligence policies that outline the process for collecting, analyzing, and sharing threat information.
- Records of threat intelligence received and shared with internal stakeholders and external partners.
- Analysis reports based on threat intelligence that inform security strategies and operations.
- Training records for security analysts on threat intelligence tools and analysis techniques.
- Membership or participation records in threat intelligence sharing platforms or industry groups.

EEE-102: Vulnerability Disclosure Management Documentation

- Vulnerability disclosure policies that define how external reports of potential vulnerabilities are managed and addressed.
- Documentation of vulnerability disclosures received, including the organization's response and remediation efforts.
- Communication records with security researchers or reporting parties regarding vulnerability disclosures.
- Reports summarizing the outcomes of vulnerability disclosures and the effectiveness of the response process.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

ID.RA-08.02: The organization has established enterprise processes to analyze disclosed vulnerabilities with a focus on:

(1) Determining its validity;

(2) Assessing its scope (e.g., affected assets);

(3) Determining it's severity and impact;

(4) Identifying affected stakeholders or customers; and

(5) Analyzing options to respond.

Subject Tags: #information_sharing | #threat_management | #vulnerability_management

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Describe how the organization has established enterprise processes to analyze disclosed vulnerabilities. Results of these analyses flow into existing risk response and exception management processes. Highlight the processes related to each of the five focus areas in the statement (validity, scope, severity and impact, affected stakeholders or customers, and options to respond).

Examples of Effective Evidence:

EEE-046: Risk Assessment and Threat Analysis Documentation

- Standardized risk assessment templates.
- Completed assessments for relevant organizational assets and processes.
- Threat analysis reports that identify potential threats and their likelihood and impact on the organization.
- Documentation of risk assessment training for staff involved in the risk management process.
- Risk registers or databases that track identified risks and their mitigation status.
- Historical trend analysis of threats and incidents to inform future risk assessments.

EEE-049: Vulnerability Disclosure and Response Protocol Documentation

- Procedures for receiving, assessing, and responding to vulnerability disclosures from external researchers, customers, or other entities.
- Communication templates and protocols for interacting with individuals or organizations reporting vulnerabilities.
- Records of disclosed vulnerabilities, including the organization's response and remediation actions.
- Agreements or MOUs with bug bounty platforms or security researchers regarding vulnerability disclosure.
- Reports summarizing the outcomes of vulnerability disclosures and the effectiveness of the response process.

EEE-102: Vulnerability Disclosure Management Documentation

- Vulnerability disclosure policies that define how external reports of potential vulnerabilities are managed and addressed.
- Documentation of vulnerability disclosures received, including the organization's response and remediation efforts.
- Communication records with security researchers or reporting parties regarding vulnerability disclosures.
- Reports summarizing the outcomes of vulnerability disclosures and the effectiveness of the response process.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

IDENTIFY / Improvement / Continuous Improvements Evaluation

ID.IM-01.01: Technology, cybersecurity, and resilience controls are regularly assessed and/or tested for design and operating effectiveness.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #resilience | #review_assessment_and_testing

Response Guidance:

Technology, cybersecurity, and resilience controls should be tested regularly to validate the design and operating effectiveness of the controls. Describe the process for ensuring controls are implemented and developed correctly and are operating as intended. Describe how the controls testing program integrates with risk assessment, exception management, and controls program assessment processes.

Provide information of testing and assessments performed to identify weaknesses and deficiencies in the control design and development process to identify areas that need improvement.

Examples of Effective Evidence:

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

EEE-050: Control Assessment and Testing Documentation

- Schedules and plans for regular assessments and testing of security controls to ensure they are functioning as intended.
- Results and reports from control assessments, including identified deficiencies and corrective actions taken.
- Documentation of testing methodologies and criteria used to evaluate the effectiveness of controls.
- Records of updates or changes to controls based on assessment findings.

ID.IM-01.02: The organization implements a regular process to collect, store, report, benchmark, and assess trends in actionable performance indicators and risk metrics (e.g., threat KRIs, security incident metrics, vulnerability metrics, and operational measures).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #enterprise_risk_management | #metrics_and_reporting | #risk_management | #risk_oversight

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

The organization should establish a risk and operational baseline and set benchmarks or target actionable performance indicators and risk metrics. A methodology should be implemented to determine if the organization is failing to meet, meeting, or exceeding those established benchmarks.

Provide information on the effectiveness of controls measured through a suite of KCI, KPI, and/or KRI that were defined and mapped to controls or operational activities. Additionally, describe the KCI/KPI/KRI formal review process and roles and needs of the various stakeholders for the reporting. Describe consistency with KCIs/KPIs/KRIs reporting across local/global business lines' countries and/or regions which are for use in governance forums.

Also provide information on how control owners (or others) assess maturity (e.g., on a scale 1-5) of controls and operational processes and the linkage to any improvement programs to uplift maturity. Define how and who independently validates the assessments.

Examples of Effective Evidence:

EEE-051: Risk Metrics and Performance Indicator Documentation

- Key performance indicators (KPIs) and risk metrics used to measure the effectiveness of the organization's risk management program.
- Dashboards or reports that track and display collected performance indicators and risk metrics.
- Documentation of the process for collecting, analyzing, and reporting on KPIs and risk metrics.
- Historical data and trend analysis used to inform risk management decisions and strategies.
- Records of management reviews or meetings where performance indicators and risk metrics are discussed and used to drive decision making or improvements.

ID.IM-01.03: The organization establishes specific objectives, performance criteria, benchmarks, and tolerance limits to identify areas that have improved or are in need of improvement over time.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #enterprise_risk_management | #mission_and_strategy | #program_transformation | #review_assessment_and_testing | #risk_management | #improvements

Response Guidance:

The organization should establish a cybersecurity baseline and set benchmarks or target performance metrics. A methodology should be implemented to determine if the organization is exceeding, just meeting, or failing to meet those established benchmarks.

Describe the technology and cybersecurity strategies and how they were developed, including the objectives and assessments to identify benchmarks and associated maturity levels. Describe how the organization identifies areas for improvement and measures the programs over time. Describe how the operational risk management framework and the three lines of defense pertain to performance criteria, benchmarks, and tolerance, including how they relate to improvement. Describe how the

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

organization agrees upon risk appetite quantitative KRIs and qualitative statements, including for information and cybersecurity risk (e.g., risk management meeting). Provide information on any review process to ensure that KRIs remain fit for purpose. Additionally, describe how the organization independently assesses external benchmarks and determines the program's maturity.

Examples of Effective Evidence:

EEE-051: Risk Metrics and Performance Indicator Documentation

- Key performance indicators (KPIs) and risk metrics used to measure the effectiveness of the organization's risk management program.
- Dashboards or reports that track and display collected performance indicators and risk metrics.
- Documentation of the process for collecting, analyzing, and reporting on KPIs and risk metrics.
- Historical data and trend analysis used to inform risk management decisions and strategies.
- Records of management reviews or meetings where performance indicators and risk metrics are discussed and used to drive decision making or improvements.

ID.IM-01.04: Technology and cybersecurity programs include elements designed to assess, manage, and continually improve the quality of program delivery in addressing stakeholder requirements and risk reduction.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #mission_and_strategy | #program_transformation | #review_assessment_and_testing | #risk_management | #improvements

Response Guidance:

Responses should describe review processes in place to assess, manage, and continually improve the quality of technology and cybersecurity programs and products in addressing stakeholder requirements and risk reduction. Describe how the organization identifies areas for improvement and measures the technology and cybersecurity program over time. Programs should integrate quality of program delivery into technology and cybersecurity programs to ensure that products are delivered fit-for-purpose and fit-for-use.

Describe performance indicators or technology and cybersecurity metrics to determine where weaknesses or gaps exist within the technology and cybersecurity programs. Describe how the organization identifies areas for improvement, assesses external benchmarks, and determines the program's maturity for overall risk reduction.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-001: Cybersecurity and IT Strategy Documents

- An integrated IT strategic plan that includes cybersecurity goals, detailing how security initiatives support and enhance long-term organizational objectives.
- Cybersecurity policy documents that are aligned with the IT strategic plan, ensuring that security measures and protocols are consistently applied across all technology projects.
- A technology and cybersecurity roadmap that provides a timeline for planned IT and security initiatives, including critical milestones and resource allocation.
- Documentation of the organization's adoption and implementation of cybersecurity frameworks demonstrating a structured approach to security practices within the strategic context.
- Consolidated IT and cybersecurity budget reports that reflect strategic financial planning for technology and security investments, highlighting the integration of cybersecurity into the overall technology and business budget.
- Strategic alignment review reports that evaluate the alignment between ongoing IT initiatives and cybersecurity objectives, ensuring that all technology projects incorporate necessary security considerations.

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

ID.IM-01.05: The organization's third-party risk management program is regularly assessed, reported on, and improved.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #mission_and_strategy | #program_transformation | #review_assessment_and_testing | #risk_management | #third_party_risk_management | #improvements | #supply_chain_management

Response Guidance:

Management should continuously assess the third-party risk management program to determine and report if gaps exists and work towards self-improvement of the program. Third-party risk management programs should work in concert with the existing enterprise risk management program.

Describe how the organization monitors the effectiveness of its third-party risk management program to reduce cyber, technology, and business risks associated with external dependencies. Describe how the organization monitors the effectiveness to reduce risk associated with third parties individually, as well as the aggregate use of third parties by the organization.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

IDENTIFY / Improvement / Tests & Exercises

ID.IM-02.01: The organization conducts regular, independent penetration testing and red team testing on the organization's network, internet-facing systems, critical applications, and associated controls to identify gaps in cybersecurity defenses.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #critical_infrastructure | #issue_management | #penetration_testing | #review_assessment_and_testing | #vulnerability_management

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Penetration testing attempts to exploit potential vulnerabilities to determine whether unauthorized access or other malicious activity is possible. The organization or an independent third-party (e.g., qualified independent contractor, internal audit) should perform penetration testing and/or red team testing (or equivalent) on the organization's network, internet-facing applications or systems, and other critical applications on existing components of the network, as well as the external network and environment. Testing may be extended on associated controls, such as physical access management.

Describe how the organization conducts periodic penetration testing and red team testing (commensurate with the nature of the threats to the organization and its assets) on the internal and external network, environment, internet-facing applications or systems, and critical applications to identify gaps in cybersecurity defenses. If an independent third-party is used, provide information on the use and scope of the third-party testing.

Examples of Effective Evidence:

EEE-036: Vulnerability Scanning and Patch Management Documentation

- Policy, standard, and/or procedure documents covering the identification, assessment, reporting, and remediation of software and device vulnerabilities, including regular patching protocols.
- Schedules and records of patch deployment activities, including system reboots, post-patch testing, dates, systems affected, and patching outcomes.
- Documentation of patching or upgrades to standard system configuration baselines.
- Reports from vulnerability scans or assessments that inform the patch management process.
- Incident reports related to vulnerabilities that were mitigated through patch management.
- Documentation and reporting of vulnerability mitigation targets.
- Records of exceptions to, assessments of, and approvals for cases where vulnerability mitigation targets or standards are not met.
- Records demonstrating the integration of patch management and change management practices.
- Approval and review documentation for patching protocols, including impact assessments and authorization records.
- Dashboards or tools used to monitor patch levels and patch application across the target environment.
- Post-implementation reviews and post-change evaluation reports assessing the impact and success of patches and any unintended consequences.
- Audit or review findings related to vulnerability management and patching practices with actions taken in response to findings.

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.
- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

EEE-085: Vulnerability Mitigation and Incident Containment Documentation

- Procedures for mitigating vulnerabilities and containing incidents to prevent further damage or data loss.
- Documentation of vulnerability scans and assessments, including identified vulnerabilities and mitigation actions taken.
- Incident containment plans, detailing specific containment strategies for different types of security incidents.
- Records of incident response drills or exercises focusing on containment and mitigation strategies.
- Post-incident reports analyzing the effectiveness of containment and mitigation efforts, with recommendations for improvement.

ID.IM-02.02: The thoroughness and results of independent penetration testing are regularly reviewed to help determine the need to rotate testing vendors to obtain fresh independent perspectives.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #penetration_testing | #review_assessment_and_testing | #vendor_management

Response Guidance:

An independent third-party (i.e., qualified independent contractor) should perform penetration testing and/or red team testing on the organization's network, internet-facing applications or systems, and other critical applications on existing components of the network. Independent penetration testing vendors should be impartial to the systems that penetration testing is performed upon.

Describe how the original regularly reviews the thoroughness and results of independent penetration test reports to help determine the need to rotate testing vendors to obtain fresh independent perspectives.

Examples of Effective Evidence:

EEE-036: Vulnerability Scanning and Patch Management Documentation

- Policy, standard, and/or procedure documents covering the identification, assessment, reporting, and remediation of software and device vulnerabilities, including regular patching protocols.
- Schedules and records of patch deployment activities, including system reboots, post-patch testing, dates, systems affected, and patching outcomes.
- Documentation of patching or upgrades to standard system configuration baselines.
- Reports from vulnerability scans or assessments that inform the patch management process.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Incident reports related to vulnerabilities that were mitigated through patch management.
- Documentation and reporting of vulnerability mitigation targets.
- Records of exceptions to, assessments of, and approvals for cases where vulnerability mitigation targets or standards are not met.
- Records demonstrating the integration of patch management and change management practices.
- Approval and review documentation for patching protocols, including impact assessments and authorization records.
- Dashboards or tools used to monitor patch levels and patch application across the target environment.
- Post-implementation reviews and post-change evaluation reports assessing the impact and success of patches and any unintended consequences.
- Audit or review findings related to vulnerability management and patching practices with actions taken in response to findings.

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.
- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.
- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

EEE-085: Vulnerability Mitigation and Incident Containment Documentation

- Procedures for mitigating vulnerabilities and containing incidents to prevent further damage or data loss.
- Documentation of vulnerability scans and assessments, including identified vulnerabilities and mitigation actions taken.
- Incident containment plans, detailing specific containment strategies for different types of security incidents.
- Records of incident response drills or exercises focusing on containment and mitigation strategies.
- Post-incident reports analyzing the effectiveness of containment and mitigation efforts, with recommendations for improvement.

ID.IM-02.03: The organization tests and validates the effectiveness of the incident detection, reporting, and communication processes and protocols with internal and external stakeholders.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #incident_management | #mission_and_strategy | #program_maturity | #risk_assessment | #risk_management | #scenario_risk_assessment | #tabletop_exercises

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

The organization should have a process in place to test incident response detection, reporting and communication processes to ensure that controls in place are effective. Incident detection processes should be tested to validate the effectiveness of the event detection, incident response processes, and controls through various exercises that emulate the types of events they are designed to detect.

Describe how the organization tests and validates the effectiveness of the incident reporting and communication processes and protocols with both internal and external stakeholders. Provide applicable assessment results (generated by the organization or a third-party) to demonstrate how the organization tested and validated the effectiveness of these processes.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

ID.IM-02.04: The organization's testing program validates the effectiveness of its resilience strategy and response, disaster recovery, and resumption plans on a regular basis or upon major changes to business or system functions, and includes external stakeholders as required.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #critical_infrastructure | #disaster_recovery | #mission_and_strategy | #program_maturity | #resilience | #risk_assessment | #risk_management | #scenario_risk_assessment | #tabletop_exercises

Response Guidance:

Describe how the organization promotes, designs, organizes, and manages testing exercises that are designed to test its resilience strategy and response, disaster recovery, and resumption plans, with participation from internal and external stakeholders as required, on a regular basis or upon major changes to business or system functions. Include information on how the organization shares results of testing exercises to the appropriate parties through metrics or board reporting.

Describe how the organization's testing program validates the effectiveness of its resilience strategy, response, disaster recovery, and resumption plans on an annual or more frequent basis according to major changes to business or system functions and the risk profile of the organization. Provide information on the organization's testing framework and strategy. Describe the types of testing performed. As referenced in ID.IM-02.05, the organization establishes testing programs should include a range of scenarios.

Examples of Effective Evidence:

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.
- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-069: Crisis Response and Business Continuity Management Documentation

- Crisis response plans that detail specific actions, communication protocols, templates, and roles during various crisis scenarios.
- Exercise and drill records, including scenarios, outcomes, and lessons learned, to validate crisis response capabilities.
- After-action reports from actual crisis events, analyzing the response effectiveness and areas for improvement.
- Stakeholder feedback on the organization's response during crisis situations, used to refine continuity and crisis response plans.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EEE-106: Recovery Objectives Critical Infrastructure Documentation

- Documentation of recovery objectives for critical infrastructure and how these align with business continuity goals.
- Critical infrastructure analysis reports that assess the resilience and recovery capabilities of essential systems.
- Records of alignment discussions or decisions between recovery objectives and business needs.
- Audit reports evaluating the alignment of recovery objectives with the criticality of infrastructure components.

EEE-107: Data Recovery and Information Flow Mapping Documentation

- Data recovery strategy documents that outline procedures for restoring lost or corrupted data.
- Information flow maps that illustrate how data moves through the organization, informing recovery planning.
- Test reports from data recovery exercises, demonstrating the ability to restore data in line with recovery strategies.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of changes to data recovery strategies based on new business processes or technologies.
- Training records for IT staff on data recovery procedures and information flow considerations.

EEE-111: Disaster Recovery and Validation Program Documentation

- Disaster Recovery (DR) plans outlining specific recovery steps for Information Technology (IT) systems and data.
- Schedules and results from regular DR testing, ensuring plans are actionable and up-to-date.
- Change management records for DR plans, capturing updates and justifications.
- Records capturing lessons-learned from exercises and the updating of documentation and plans to reflect the improvements.
- Training and certification records for personnel on DR roles and procedures.
- Review reports assessing DR plan alignment with overall business recovery objectives and Business Impact Analyses (BIAs).

ID.IM-02.05: The organization establishes testing programs that include a range of scenarios, including severe but plausible scenarios (e.g., disruptive, destructive, corruptive), that could affect the organization's ability to service internal and external stakeholders.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #critical_infrastructure | #disaster_recovery | #incident_management | #mission_and_strategy | #program_maturity | #resilience | #risk_assessment | #risk_management | #scenario_risk_assessment | #tabletop_exercises | #threat_landscape | #threat_management

Response Guidance:

Describe how the organization establishes testing programs based on the risk profile of the organization business impact analyses, and resilience risk analyses.

Describe how the testing programs include a range of scenarios, including severe but plausible scenarios (e.g., disruptive, destructive, corruptive) that could affect the organization's ability to service internal and external stakeholders. These scenarios should have a range of cyber, environmental, third-party, and business scenarios.

Examples of Effective Evidence:

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.
- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-069: Crisis Response and Business Continuity Management Documentation

- Crisis response plans that detail specific actions, communication protocols, templates, and roles during various crisis scenarios.
- Exercise and drill records, including scenarios, outcomes, and lessons learned, to validate crisis response capabilities.
- After-action reports from actual crisis events, analyzing the response effectiveness and areas for improvement.
- Stakeholder feedback on the organization's response during crisis situations, used to refine continuity and crisis response plans.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EEE-111: Disaster Recovery and Validation Program Documentation

- Disaster Recovery (DR) plans outlining specific recovery steps for Information Technology (IT) systems and data.
- Schedules and results from regular DR testing, ensuring plans are actionable and up-to-date.
- Change management records for DR plans, capturing updates and justifications.
- Records capturing lessons-learned from exercises and the updating of documentation and plans to reflect the improvements.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Training and certification records for personnel on DR roles and procedures.
- Review reports assessing DR plan alignment with overall business recovery objectives and Business Impact Analyses (BIAs).

ID.IM-02.06: The organization designs and tests its systems and processes<font

color="#171717">, and employs third-party support resources (e.g., Sheltered Harbor), to enable recovery of accurate data (e.g., material financial transactions) sufficient to support defined business recovery time and recovery point objectives.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #critical_infrastructure | #disaster_recovery | #mission_and_strategy | #program_maturity | #resilience | #risk_assessment | #risk_management | #scenario_risk_assessment | #tabletop_exercises

Response Guidance:

Describe how the organization designs and tests its systems and processes, and employs third-party support resources to enable recovery of data (e.g., material financial transactions) sufficient to support defined business recovery time and recovery point objectives. For example, an organization can use Sheltered Harbor for third party support to securely store and quickly restore data and services to meet business recovery time and recovery point objectives. Describe how the organization designs requirements for backups and replications of data based on data sensitivity and criticality. Describe how the organization employs third party support resources to enable recovery of accurate data. Provide information regarding systems and processes risk classification as it pertains to design and testing frequency. Provide information on the types of backups utilized based upon the risk classification.

Examples of Effective Evidence:

EEE-106: Recovery Objectives Critical Infrastructure Documentation

- Documentation of recovery objectives for critical infrastructure and how these align with business continuity goals.
- Critical infrastructure analysis reports that assess the resilience and recovery capabilities of essential systems.
- Records of alignment discussions or decisions between recovery objectives and business needs.
- Audit reports evaluating the alignment of recovery objectives with the criticality of infrastructure components.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

ID.IM-02.07: The organization's governing body (e.g., the Board or one of its committees) and senior management are involved in testing as part of a crisis management team and are informed of test results.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #critical_infrastructure | #disaster_recovery | #mission_and_strategy | #program_maturity | #resilience | #risk_assessment | #risk_management | #risk_oversight | #scenario_risk_assessment | #tabletop_exercises

Response Guidance:

Tabletop exercises are a common way of involving senior leaders in resilience plan testing activities. Describe how the organization’s governing body and senior management are involved in testing as part of a crisis management team. Provide information on how the organization’s governing body is informed of test results. Provide information related to the integration of the Board and relevant committees and senior management in the process.

Examples of Effective Evidence:

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-062: Board Oversight and Risk Management Documentation

- Minutes from board meetings where risk management reviews are conducted, demonstrating oversight.
- Risk management review reports that are presented to the board, including findings and recommendations.
- Policies that define the board's role in overseeing risk management activities.
- Records of board-directed actions taken in response to risk management reviews.
- Training materials for board members on risk management principles and their oversight responsibilities.

ID.IM-02.08: The organization tests and exercises, independently and in coordination with other critical sector partners, its ability to support sector-wide resilience in the event of extreme financial stress or the instability of external dependencies, such as connectivity to markets, payment systems, clearing entities, messaging services, etc.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Subject Tags: #critical_infrastructure | #dependency_management | #disaster_recovery | #information_sharing | #mission_and_strategy | #resilience | #risk_assessment | #risk_management | #scenario_risk_assessment | #tabletop_exercises

Response Guidance:

Testing the resilience of operations and services helps identify potential threats to the ongoing performance of the operation or service. A prolonged disruption of a significant operation could generate systemic risk. Describe how the organization tests and exercises, independently and in coordination with other critical sector partners, its cyber resilience plans, to support financial sector's sector-wide resilience and address external dependencies. Highlight external dependencies, such as connectivity to markets, payment systems, clearing entities, messaging services, etc.

Examples of Effective Evidence:

EEE-015: Sector-Wide Dependency and Impact Analysis Documentation

- Analysis reports detailing the dependencies within the organization's sector and potential vulnerabilities.
- Tools or software used to evaluate the criticality of external partners and suppliers.
- Summaries from workshops and exercises aimed at understanding the sector-wide impact of external disruptions.
- Reports on how regulatory changes could affect critical external dependencies.
- Real-time dashboards for monitoring geopolitical events that may impact the sector.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

ID.IM-02.09: Corrective actions for gaps identified during security-related, incident management, response plan, and disaster recovery testing are retested and validated, or have a formal risk acceptance or risk exception.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #critical_infrastructure | #disaster_recovery | #issue_management | #mission_and_strategy | #program_transformation | #resilience | #review_assessment_and_testing | #risk_management | #risk_oversight | #tabletop_exercises

Response Guidance:

Describe periodic testing and exercises using plausible scenarios to identify weaknesses and gaps in incident management, response plan, and disaster recovery plans. Describe how the organization develops corrective actions for gaps identified during tests and exercises. Corrective actions should be retested and validated or have a formal risk acceptance or a risk exception that is reviewed and approved by management.

Provide information on how corrective actions are tracked to closure for gaps identified. Provide information on how remediation is retested and validated.

Examples of Effective Evidence:

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.
- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.
- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

EEE-048: Exception Management and Vulnerability Handling Documentation

- Policies and procedures for handling exceptions to standard security policies, including the process for requesting and approving exceptions.
- Documentation of approved policy exceptions, including justification, risk assessment, and compensating controls.
- Vulnerability exception records that detail the rationale for not remediating certain vulnerabilities and the associated risk acceptance.
- Audit reports that review the management of policy and vulnerability exceptions.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

IDENTIFY / Improvement / Improvements from Lessons Learned

ID.IM-03.01: A formal process is in place to improve protection controls and processes by integrating recommendations, findings, and lessons learned from exercises, testing, audits, assessments, and incidents.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #incident_management | #issue_management | #lessons_learned | #risk_management

Response Guidance:

Lessons learned analysis is a key element of continuous improvement in cybersecurity preparedness.

Provide information on the formal process utilized to improve protection controls and processes by integrating recommendations, findings, and lessons learned from exercises, testing, audits, assessments, and incidents. Describe any tools and industry mapping utilized in support. Provide evidence of updates to protection processes through lessons learned activities or other analysis.

Examples of Effective Evidence:

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

EEE-050: Control Assessment and Testing Documentation

- Schedules and plans for regular assessments and testing of security controls to ensure they are functioning as intended.
- Results and reports from control assessments, including identified deficiencies and corrective actions taken.
- Documentation of testing methodologies and criteria used to evaluate the effectiveness of controls.
- Records of updates or changes to controls based on assessment findings.

ID.IM-03.02: The organization establishes a systematic and comprehensive program to regularly evaluate and improve its monitoring and detection processes and controls as the threat environment changes, tools and techniques evolve, and lessons are learned.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #issue_management | #lessons_learned | #risk_management | #security_logging_monitoring_and_alerting | #threat_landscape

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

One of the most important parts of incident response is learning and improving. Holding a "lessons learned" meeting with all involved parties after incidents can be extremely helpful in improving security measures and the incident handling process itself.

Describe the program used to regularly evaluate and improve the monitoring and detection processes and controls. Describe how lessons learned are incorporated as the threat environment landscape changes, and tools and techniques evolve. Provide information on the linkage to the overall incident management process.

Examples of Effective Evidence:

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.
- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.
- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

IDENTIFY / Improvement / Plans Affecting Operations

ID.IM-04.01: The organization's business continuity, disaster recovery, crisis management, and response plans are in place and managed, aligned with each other, and incorporate considerations of cyber incidents.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #disaster_recovery | #issue_management | #mission_and_strategy | #program_maturity | #resilience | #risk_assessment | #risk_management | #risk_oversight

Response Guidance:

The organization should have approved business continuity, disaster recovery, crisis management, and response plans in place to recover operations following an incident. The organization should have plans in place that address business impact analysis and risk assessment, alternate processing for critical business functions while systems/applications and facilities are unavailable. The organization should establish recovery strategies and procedures for critical systems, roles and responsibilities, and business continuity and disaster recovery testing that are managed and aligned with each other. Plans should be integrated and aligned to prepare an organization to continue critical business services during disruption.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Describe how the organization's business continuity (business process), disaster recovery (data center process), crisis management (business process), and incident response plans (incident process) are in place, coordinated, managed, aligned with each other, and incorporate considerations of cyber incidents.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EEE-106: Recovery Objectives Critical Infrastructure Documentation

- Documentation of recovery objectives for critical infrastructure and how these align with business continuity goals.
- Critical infrastructure analysis reports that assess the resilience and recovery capabilities of essential systems.
- Records of alignment discussions or decisions between recovery objectives and business needs.
- Audit reports evaluating the alignment of recovery objectives with the criticality of infrastructure components.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-111: Disaster Recovery and Validation Program Documentation

- Disaster Recovery (DR) plans outlining specific recovery steps for Information Technology (IT) systems and data.
- Schedules and results from regular DR testing, ensuring plans are actionable and up-to-date.
- Change management records for DR plans, capturing updates and justifications.
- Records capturing lessons-learned from exercises and the updating of documentation and plans to reflect the improvements.
- Training and certification records for personnel on DR roles and procedures.
- Review reports assessing DR plan alignment with overall business recovery objectives and Business Impact Analyses (BIAs).

ID.IM-04.02: The organization's incident response and business continuity plans contain clearly defined roles, responsibilities, and levels of decision-making authority, and include all needed areas of participation and expertise across the organization and key third-parties.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #incident_management | #policy_management | #resilience | #risk_oversight

Response Guidance:

Describe how the organization's incident response plan and business continuity plans contain clearly defined roles, responsibilities, and levels of decision-making authority. The organization may use RACI charts to define leadership, ownership, and accountability of specific roles and responsibilities to ensure all needed areas of participation and expertise are included from internal and external stakeholders. The organization's incident response plan and business continuity plan should include details on decision making authority and escalation procedures.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

ID.IM-04.03: Recovery plans include service resumption steps for all operating environments, including traditional, alternate recovery, and highly available (e.g., cloud) infrastructures.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #architecture | #disaster_recovery | #incident_management | #resilience

Response Guidance:

The organization should evaluate critical business services and processes to determine a process for recovery of traditional, alternate recovery, and highly available infrastructures based on the organization. Organizations are accountable for ensuring that even highly available infrastructure, such as cloud-based infrastructure, is recoverable. Demonstrate the recovery plan includes service resumption steps for all operating environments, including traditional, alternate recovery, and highly available (e.g., cloud) infrastructures.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.
- Business continuity plan outlining procedures for maintaining service delivery during disruptions.
- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.
- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.
- Contingency plans detailing alternative service delivery methods.
- Training records for staff on resilience and continuity procedures and their roles during incidents.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EEE-106: Recovery Objectives Critical Infrastructure Documentation

- Documentation of recovery objectives for critical infrastructure and how these align with business continuity goals.
- Critical infrastructure analysis reports that assess the resilience and recovery capabilities of essential systems.
- Records of alignment discussions or decisions between recovery objectives and business needs.
- Audit reports evaluating the alignment of recovery objectives with the criticality of infrastructure components.

ID.IM-04.04: The organization has plans to identify, in a timely manner, the status of all transactions and member positions at the time of a disruption, supported by corresponding recovery point objectives.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #disaster_recovery | #incident_management | #security_logging_monitoring_and_alerting

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Describe what the organization has in place to identify, in a timely manner, the status of all transactions and member positions at the time of a disruption, consistent with the organization's recovery point objectives, the point in time to which data must be recovered. Provide information on how assets are classified, and risks are assessed in support of transaction identification, backup, and recovery strategy.

Examples of Effective Evidence:

EEE-016: Recovery Objectives and Strategic Alignment Documentation

- Tools and templates used for formulating recovery strategies that support business objectives.
- A matrix aligning recovery time and point objectives with business priorities.
- Documentation from strategic planning sessions focused on recovery objectives.
- Signed approvals from management endorsing the proposed recovery strategies.
- Periodic review reports assessing the alignment of recovery objectives with business needs.

EEE-106: Recovery Objectives Critical Infrastructure Documentation

- Documentation of recovery objectives for critical infrastructure and how these align with business continuity goals.
- Critical infrastructure analysis reports that assess the resilience and recovery capabilities of essential systems.
- Records of alignment discussions or decisions between recovery objectives and business needs.
- Audit reports evaluating the alignment of recovery objectives with the criticality of infrastructure components.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

ID.IM-04.05: Recovery plans include restoration of resilience following a long term loss of capability (e.g., at an alternate site or a third-party), detailing when the plan should be activated and implementation steps.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #architecture | #critical_infrastructure | #data_backup | #disaster_recovery | #hotswap | #incident_management | #resilience | #technology_availability

Response Guidance:

The organization's recovery plan should address and incorporate how the organization will maintain resilience following a long-term loss of capability. For example, the organization should establish an agreed-upon protocol between the organization and third parties for determining how incidents will be handled to maintain resilience.

Demonstrate the recovery plan includes restoration of resilience and recovery of services following a long-term loss of capability (e.g., site or third party) detailing when the plan should be activated and how it is to be implemented. Highlight activation triggers and implementation steps.

Examples of Effective Evidence:

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.
- Business continuity plan outlining procedures for maintaining service delivery during disruptions.
- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.
- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.
- Contingency plans detailing alternative service delivery methods.
- Training records for staff on resilience and continuity procedures and their roles during incidents.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EEE-106: Recovery Objectives Critical Infrastructure Documentation

- Documentation of recovery objectives for critical infrastructure and how these align with business continuity goals.
- Critical infrastructure analysis reports that assess the resilience and recovery capabilities of essential systems.
- Records of alignment discussions or decisions between recovery objectives and business needs.
- Audit reports evaluating the alignment of recovery objectives with the criticality of infrastructure components.

EEE-111: Disaster Recovery and Validation Program Documentation

- Disaster Recovery (DR) plans outlining specific recovery steps for Information Technology (IT) systems and data.
- Schedules and results from regular DR testing, ensuring plans are actionable and up-to-date.
- Change management records for DR plans, capturing updates and justifications.
- Records capturing lessons-learned from exercises and the updating of documentation and plans to reflect the improvements.
- Training and certification records for personnel on DR roles and procedures.
- Review reports assessing DR plan alignment with overall business recovery objectives and Business Impact Analyses (BIAs).

ID.IM-04.06: The organization has established and implemented plans to identify and mitigate the cyber risks it poses through interconnectedness to sector partners and external stakeholders.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Subject Tags: #enterprise_risk_management | #information_sharing | #mission_and_strategy | #risk_management | #threat_management

Response Guidance:

Cyber-risk, threat, and events impacting an organization can proliferate to the systems of other organizations due to the interconnectivity among systems. Describe how the organization has established and implemented plans to identify and mitigate the cyber risks it poses through interconnectedness to sector partners and external stakeholders.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

ID.IM-04.07: The organization pre-identifies, pre-qualifies, and retains third party incident management support and forensic service firms, as required, that can be called upon to quickly assist with incident response, investigation, and recovery.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #incident_management | #third_party_risk_management | #vendor_management | #supply_chain_management

Response Guidance:

Describe processes for an organization pre-identifying, pre-qualifying, and retaining third party support to effectively prepare and respond to an incident in a timely manner. Organizations should develop and prepare for potential incidents by developing an incident response management plan that is periodically tested (e.g., scenario planning, tabletops, etc.) with the participation of third parties. Response roles and responsibilities should be defined for internal and external individuals to ensure an organization is able to quickly and effectively assist with incident response, forensic, investigation, and recovery.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-021: Third-Party Cybersecurity and Continuity Assessment Documentation

- Reports from cybersecurity assessments conducted on third-party vendors, including findings and recommendations.
- Third-party business continuity plans that detail recovery strategies and objectives relevant to services provided (or records of plan reviews).
- Agreements with third parties that include requirements for cybersecurity measures and business continuity planning.
- Documentation of joint business continuity exercises with critical vendors, including outcomes and improvements.
- Vendor cybersecurity certification records, verifying adherence to industry standards and best practices.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

ID.IM-04.08: The organization regularly reviews response strategy, incident management plans, recovery plans, and associated tests and exercises and updates them, as necessary, based on:

(1) Lessons learned from incidents that have occurred (both internal and external to the organization);

(2) Current cyber threat intelligence (both internal and external sources);

(3) Recent and wide-scale cyber attack scenarios;

(4) Operationally and technically plausible future cyber attacks;

(5) Organizational or technical environment changes; and,

(6) New technological developments.

Subject Tags: #disaster_recovery | #emerging_technologies | #incident_management | #lessons_learned | #mission_and_strategy | #program_maturity | #risk_assessment | #risk_management | #scenario_risk_assessment | #tabletop_exercises | #threat_landscape | #threat_management

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Describe how the organization periodically reviews response strategy, incident management plans, recovery plans, and associated test and exercises and updates them as necessary based on the six criteria within the statement (lessons learned, cyber threat intelligence, recent cyber-attacks, future cyber-attacks, environment changes, and new technology).

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-050: Control Assessment and Testing Documentation

- Schedules and plans for regular assessments and testing of security controls to ensure they are functioning as intended.
- Results and reports from control assessments, including identified deficiencies and corrective actions taken.
- Documentation of testing methodologies and criteria used to evaluate the effectiveness of controls.
- Records of updates or changes to controls based on assessment findings.

EEE-084: Cyber Threat Intelligence Sharing and Distribution Documents

- Policies and procedures for collecting, analyzing, and distributing cyber threat intelligence within the organization and with external partners.
- Agreements or memberships with threat intelligence sharing platforms or industry groups.
- Records of threat intelligence briefings or alerts issued to relevant stakeholders.
- Evaluations of the threat intelligence program, assessing its contribution to the organization's security posture.

EEE-101: Cyber Threat Intelligence Sharing Documentation

- Cyber threat intelligence policies that outline the process for collecting, analyzing, and sharing threat information.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of threat intelligence received and shared with internal stakeholders and external partners.
- Analysis reports based on threat intelligence that inform security strategies and operations.
- Training records for security analysts on threat intelligence tools and analysis techniques.
- Membership or participation records in threat intelligence sharing platforms or industry groups.

PROTECT / Identity Management, Authentication, and Access Control / Identity & Credential Management

PR.AA-01.01: Identities and credentials are actively managed or automated for authorized devices and users (e.g., removal of default and factory passwords, password strength requirements, automatic revocation of credentials under defined conditions, regular asset owner access review, etc.).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authentication | #authorization | #credential_management | #identity_and_access_management

Response Guidance:

The goal of access control is to allow access by authorized individuals and devices and to disallow access by all others. Role-based access control may be considered to simplify management activities. Access should be authorized and provided only to individuals whose identity is established, and their activities should be limited to the minimum required for business purposes. Asset owners should regularly review access roles and individuals authorized to access the system to verify appropriate access management procedures.

Access controls should include password complexity, limitation of the number of password attempts before a user is locked out, and prohibition of the reuse of passwords. The organization should create complex passwords for default administration passwords, otherwise the network may be vulnerable to attack or employee abuse. Default passwords should be changed per system implementation guidelines, change management procedures or system hardening documentation.

Changes to access privileges of critical systems should be continuously monitored and any changes to those access privileges should result in an alert and notification to the proper security team to investigate, document, and resolve any issues. Where possible, access management activities should be automated to reduce error and manual processing overhead. Access management policies and procedures should establish a process for terminating users. If an organization terminates an individual's employment, there should be measures in place that require that user's access to any asset or system be removed immediately.

Provide information in support of identities and credentials being actively managed and/or automated for authorized devices and users.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

PR.AA-01.02: Physical and logical access to systems is permitted only for individuals who have a legitimate business requirement, have been authorized, and who are adequately trained and monitored.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authorization | #identity_and_access_management | #least_privileged_access | #physical_security | #training_and_awareness

Response Guidance:

The organization's management should ensure all users are identified and authenticated when accessing systems, applications, and hardware. Asset owners should determine the appropriate persons to allow access to and the types of access roles in place at the organization.

Provide information regarding the physical and logical access controls that demonstrate that access is only permitted to individuals who have a legitimate business requirement, have been authorized, and who are adequately trained and monitored. Describe the request and review process and how that supports the statement. Describe the training and monitoring conducted for users, particularly those with access to sensitive and/or critical data.

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PROTECT / Identity Management, Authentication, and Access Control / Identity Binding to Credentials

PR.AA-02.01: The organization authenticates identity, validates the authorization level of a user before granting access to its systems, limits the use of an account to a single individual, and attributes activities to the user in logs and transactions.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authentication | #authorization | #credential_management | #identity_and_access_management | #security_logging_monitoring_and_alerting

Response Guidance:

The organization's management should ensure all users are identified and authenticated when accessing systems, applications, and hardware. Identification of a user is commonly associated with a user account name or other identifier, such as a unique identifier, account number, or email address.

Provide information on how the organization authenticates identity, validates the authorization level of a user before granting access to its systems, limits the use of an account to a single individual, and attributes activities to the user in logs and transactions. Provide information on authentication methods (e.g., MFA) determined by the risk of the user and/or transaction type. Describe how the organization attributes activities to the user in logs and transactions. For example, a process in place to record the ID of the user performing a transaction in all logs and application records to accurately recreate the activity.

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PROTECT / Identity Management, Authentication, and Access Control / Authentication

PR.AA-03.01: Based on the risk level of a user access or a specific transaction, the organization defines and implements authentication requirements, which may include multi-factor or out-of-band authentication, and may adopt other real-time risk prevention or mitigation tactics.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authentication | #authorization | #credential_management | #identity_and_access_management | #multi_factor_authentication | #risk_management

Response Guidance:

The organization should conduct risk assessments and use effective authentication methods appropriate to the level of risk of a given transaction, user access, or connection. Best practices include: selecting authentication mechanisms based on the risk associated with the particular application or service; considering whether multi-factor authentication is appropriate for each application; and encrypting the transmission and storage of authenticators (e.g., passwords, personal identification numbers (PINs), digital certificates, and biometric templates).

Describe how, based on the risk level of a given transaction, user access, or connection, the organization has defined and implemented appropriate authentication requirements.

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

PR.AA-03.02: Decisions to authorize user access to devices and other assets are made with consideration of:

(1) Business need for the access;

(2) The type of data being accessed (e.g., customer PII, public data);

(3) The risk of the transaction (e.g., internal-to-internal, external-to-internal);

(4) The organization's level of trust for the accessing agent (e.g., external application, internal user); and

(5) The potential for harm.

Subject Tags: #authentication | #authorization | #identity_and_access_management | #least_privileged_access | #privileged_access

Response Guidance:

Provide information on how the organization performs decisions to authorize user access to devices and other assets. Risk assessments may be performed to help the organization identify high-risk devices or assets. Connections within the organization can be internal or external. For example, VPN, third parties, network segments, or leased lines. Describe how the assessment considers the business need for the access, type of data being accessed, the risk of the transaction or connection within or to the ecosystem, the organization's level of trust, and the potential for harm. Provide information on the asset owner's role in analysis and decision to authorize user access to devices and other assets.

Examples of Effective Evidence:

EEE-007: Legal, Regulatory, and Compliance Management Documentation

- Compliance audit reports for relevant laws and regulations (e.g., GDPR, HIPAA).
- Documentation of legal advice received on cybersecurity matters, to include determinations of incident materiality.
- Records of regulatory filings and notices related to IT and cybersecurity.
- Updates to policies and procedures in response to legal and regulatory changes.
- Training records on legal and regulatory requirements for IT staff.

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of user account creation, modification, and termination processes.

PR.AA-03.03: The organization reduces fraudulent activity and protects reputational integrity through email verification mechanisms (e.g., DMARC, DKIM), call-back verification, secure file exchange facilities, out-of-band communications, customer outreach and education, and other tactics designed to thwart imposters and fraudsters.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authentication | #fraud | #identity_and_access_management | #program_maturity

Response Guidance:

Address spoofing, phishing, and man-in-the-middle attacks are common email exploits that can damage the reputational integrity of an organization. Responses should include an organization's email verification mechanisms such as Domain-based Message Authentication, Reporting, and Conformance (DMARC), Domain Keys Identified Mail (DKIM), call-back verification, secure file exchange facilities, out-of-band communications, customer outreach and education, or similar authentication protocol mechanisms implemented to protect email confidentiality and reputational integrity.

Describe which email verification mechanisms have been implemented to reduce fraudulent activity and thwart imposters and fraudsters. Provide information on the mechanisms utilized.

Examples of Effective Evidence:

EEE-039: Malware Protection and Incident Detection Documentation

- Anti-malware policies and procedures, including strategies for prevention, detection, and response.
- Logs from anti-malware solutions showing coverage, detection, and remediation of malicious software.
- Exception reports and tracking of malware detection failures and gaps.
- Incident response plans that include specific protocols for handling malware-related incidents.
- Post-incident analysis reports that evaluate the effectiveness of malware protection strategies.

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.
- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Streamlined training documentation for all employees on data protection and encryption best practices.

EEE-075: Malware and Mobile Code Defense Strategy Documents

- Policies and procedures for defending against malware and malicious mobile code, including prevention, detection, and response strategies.
- Configuration records for anti-malware tools and systems, showing protective measures in place.
- Logs and reports from anti-malware solutions, documenting detections and actions taken.
- Post-incident analysis documents that evaluate the response to malware incidents and the effectiveness of defense mechanisms.

EEE-109: Email Protection Mechanism Documents

- Policies and procedures for securing email communications, including spam filters, phishing detection, and encryption.
- Configuration records for email protection systems, demonstrating the implementation of security measures.
- Training records for employees on recognizing and reporting suspicious emails and following email security best practices.
- Incident logs related to email security threats, including actions taken and resolutions.
- Audit or review reports assessing the effectiveness of email protection mechanisms and identifying areas for improvement.

PROTECT / Identity Management, Authentication, and Access Control / Identity Assertions

PR.AA-04.01: Access credential and authorization mechanisms for internal systems and across security perimeters (e.g., leveraging directory services, directory synchronization, single sign-on, federated access, credential mapping, etc.) are designed to maintain security, integrity, and authenticity.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authentication | #authorization | #credential_management | #identity_and_access_management

Response Guidance:

As referenced in PR.AA. Responses should ensure that authorized personnel have credentials and authentication mechanisms in place for physical and logical access, specific to their job duties, and while implementing least privilege access for internal systems and across security perimeters. Authorization mechanisms should be in place to centralize access control including directory services, directory synchronization, single sign-on, federated access, credential mapping, etc.). Refer to DE.CM-06.01, the organization should have processes to review, document, and authorize, all third-party connections, data transfer mechanisms, and Application Programming Interfaces (APIs).

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Describe authorization mechanisms that are implemented and designed to maintain security, integrity, and authenticity.

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

PROTECT / Identity Management, Authentication, and Access Control / Access Authorizations

PR.AA-05.01: The organization limits access privileges to the minimum necessary and with consideration of separation of duties (e.g., through role-based access control, asset owner access recertifications, etc.).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authorization | #least_privileged_access | #separation_of_duties

Response Guidance:

Least privilege refers to allowing only authorized access for users which are necessary to accomplish the assigned tasks in accordance with organizational missions and business functions. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. The organization should limit access privileges with consideration of separation of duties by only granting access needed to perform an individual's role and responsibilities.

Responses should ensure that authorized personnel have credentials and authentication mechanisms in place for physical and logical access, specific to their job duties, and while implementing least privilege access for internal systems and across security perimeters. Authorization mechanisms should be in place to centralize access control including directory services, directory synchronization, single sign-on, federated access, credential mapping, etc.) Describe authorization mechanisms that are implemented and designed to maintain security, integrity, and authenticity.

Provide information regarding how the organization limits access privileges to the minimum necessary and with consideration of separation of duties.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

EEE-066: Segregation of Duties in Risk Management Documentation

- Policies and procedures that establish segregation of duties within risk management activities to prevent conflicts of interest and fraud.
- Flowcharts or diagrams that illustrate the separation of roles and responsibilities in risk-related processes.
- Internal control reports that verify the effectiveness of segregation of duties in mitigating risks.
- Records of changes to duties or responsibilities to maintain proper segregation as the organization evolves.

PR.AA-05.02: The organization institutes controls over privileged system access by strictly limiting and closely managing staff and services with elevated system entitlements (e.g., multi-factor authentication, dual accounts, privilege and time constraints, etc.)

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #access_management | #authentication | #authorization | #credential_management | #identity_and_access_management | #multi_factor_authentication | #privileged_access | #session_management

Response Guidance:

The organization should provide the necessary reviews and authorization (approval) for privileged access when necessary. Good practices for controlling privileged access include: identifying each privilege associated with each system component, implementing a process to allocate privileges and allocating those privileges either on a need-to-use or an event-by-event basis, documenting the granting and administrative limits on privileges, and finding alternate ways of achieving the business objectives, among other practices. Management should implement database access controls that help prevent unauthorized download or transmission of confidential data. Managers of persons with privileged access should understand the nature of the access required and be able to identify appropriate and inappropriate activity.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Provide information on how the organization institutes controls over privileged system access by strictly limiting and closely managing staff and services with elevated system access entitlements. Describe the risk-based approach and frameworks in place.

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

PR.AA-05.03: The organization institutes controls over service account (i.e., accounts used by systems to access other systems) lifecycles to ensure strict security over creation, use, and termination; access credentials (e.g., no embedded passwords in code); frequent reviews of account ownership; visibility for unauthorized use; and hardening against malicious insider use.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #access_management | #credential_management | #identity_and_access_management | #policy_management | #privileged_access

Response Guidance:

The organization should develop security standards based on industry configuration guidelines that establish specific baseline security controls.

Provide information on how the organization institutes controls over service accounts, including third party connections. Refer to DE.CM-06.01, for how the organization should authorize third party connections. Provide information on the lifecycle framework in place to ensure strict security over creation, use, and termination of access credentials, reviews of account ownership, visibility for authorized use, and hardening against malicious insider use. For example, when service accounts are retired, the associated credentials should also be returned. If not controlled and restricted to authorized users, service accounts may impact network performance and disable key controls.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

PR.AA-05.04: Specific roles, responsibilities, and procedures to manage the risk of third-party access to organizational systems and facilities are defined and implemented.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #access_management | #identity_and_access_management | #policy_management | #third_party_risk_management | #supply_chain_management

Response Guidance:

A third-party security policy or vendor management policy may assign specific roles and responsibilities to manage the risk of third-party access to the organization's system and facilities. Describe how specific roles, responsibilities, and procedures for third-party risk management are defined and implemented by the organization. As needed, restrictions or controls for third-party access to systems (i.e., for individuals and service accounts) are addressed in contracts and agreements.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

PROTECT / Identity Management, Authentication, and Access Control / Physical Access

PR.AA-06.01: The organization manages, protects, and logs physical access to sensitive areas, devices, consoles, equipment, and network cabling and infrastructure.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #asset_management | #facilities_management | #identity_and_access_management | #physical_access | #physical_infrastructure | #security_logging_monitoring_and_alerting

Response Guidance:

The organization should log and monitor the physical environment (e.g., entrances, restricted areas, confidential data repositories, vault areas, and ATMs) to prevent unauthorized access attempts and enable response efforts.

Implementing appropriate preventative and detective physical controls protects systems, data, employees, and infrastructure against malicious or unauthorized persons. Sessions on systems and applications that handle sensitive customer data should have controls in place to lock or close the session and require users to re-authenticate (e.g., security settings or parameters for inactivity in Windows Active Directory and the core processing system).

Describe how the organization manages, protects, and logs physical access to sensitive areas, devices, consoles, equipment, and network cabling and infrastructure.

Examples of Effective Evidence:

EEE-077: Physical and Environmental Security Documents

- Documentation of environmental controls (e.g., fire suppression, climate control) and physical security measures (e.g., access controls, surveillance systems).
- Maintenance and inspection records for environmental and physical security equipment.
- Incident logs related to environmental hazards or physical security breaches, including responses and outcomes.
- Security audit reports evaluating the adequacy of environmental and physical security controls.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PR.AA-06.02: The organization manages and protects physical and visual access to sensitive information assets and physical records (e.g., session lockout, clean desk policies, printer/facsimile output trays, file cabinet/room security, document labelling, etc.)

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #data_protection | #facilities_management | #physical_access | #policy_management | #session_management

Response Guidance:

Provide information on physical and visual access controls implemented according to the assets at risk (e.g., data, infrastructure, systems). Responses should have physical and environmental policies, standards, and procedures in place that are aligned to the organization's risk management strategy and framework.

Describe how the organization develops and manages individuals with authorized access to the organization's facilities. Describe how the organization issues credentials for facility access, disables sessions after an established period of inactivity (e.g., session lockout), and monitors physical access. Training materials should be employed to ensure personnel are informed of clean desk policies, file cabinet/room security, document labelling, and printer/facsimile output tray procedures.

Examples of Effective Evidence:

EEE-077: Physical and Environmental Security Documents

- Documentation of environmental controls (e.g., fire suppression, climate control) and physical security measures (e.g., access controls, surveillance systems).
- Maintenance and inspection records for environmental and physical security equipment.
- Incident logs related to environmental hazards or physical security breaches, including responses and outcomes.
- Security audit reports evaluating the adequacy of environmental and physical security controls.

PROTECT / Awareness and Training / User Awareness & Training

PR.AT-01.01: All personnel receive cybersecurity awareness training upon hire and on a regular basis.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #training_and_awareness

Response Guidance:

The organization should have a cybersecurity training program designed to increase employees' situational awareness of cybersecurity threats and knowledge of cybersecurity controls. As referenced, in PR.AT-01.02, training should support topics of situational awareness and competencies for data protection, personal data handling, compliance obligations, working with third

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

parties, detecting cyber risks, and how to report any unusual activity or incidents. Organizations should maintain a record of all training received.

Provide situational awareness training that is relevant to all personnel (full-time or part-time; permanent, temporary or contract) upon hire and on a regular basis. Prescribed training should be scoped and defined for areas where additional job-relevant requirements warrant additional validation. Provide information on any exceptions.

As referenced in PR.AT-01.03, training should be updated on a regular basis to reflect the risks and threats identified by the organization, the organization's security policies and standards, applicable laws and regulations, and changes in individual responsibilities.

Examples of Effective Evidence:

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.
- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

EEE-043: Cybersecurity Training, Awareness, and Expertise Access Documentation

- Agendas and materials from cybersecurity awareness events and training sessions.
- Records of accessing/retaining cybersecurity expertise and resources, including external consultants or internal experts.
- Partnerships with educational institutions or professional organizations to enhance cybersecurity knowledge.
- Records of employee participation in external cybersecurity conferences, workshops, or courses.
- Feedback from employees on the accessibility and usefulness of cybersecurity training and expertise.

PR.AT-01.02: Cybersecurity awareness training includes, at a minimum, awareness of and competencies for data protection, personal data handling, compliance obligations, working with third parties, detecting cyber risks, and how to report any unusual activity or incidents.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #compliance | #data_protection | #incident_management | #review_assessment_and_testing | #third_party_risk_management | #training_and_awareness | #supply_chain_management

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

The organization should have an organizational-wide information security training program designed to increase workforce situational awareness of information security threats and demonstrate minimum required knowledge of information security controls. The training program should consider the evolving and persistent threats and should include annual certification that personnel understand their responsibilities. Training can be provided by the organization or by a third-party training provider.

Provide information as to what is included in the cybersecurity situational awareness training plan. Provide information that supports the training topics of situational awareness and competencies for data protection, personal data handling, compliance obligations, working with third parties, detecting cyber risks, and how to report any unusual activity or incidents.

Examples of Effective Evidence:

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.
- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

EEE-043: Cybersecurity Training, Awareness, and Expertise Access Documentation

- Agendas and materials from cybersecurity awareness events and training sessions.
- Records of accessing/retaining cybersecurity expertise and resources, including external consultants or internal experts.
- Partnerships with educational institutions or professional organizations to enhance cybersecurity knowledge.
- Records of employee participation in external cybersecurity conferences, workshops, or courses.
- Feedback from employees on the accessibility and usefulness of cybersecurity training and expertise.

EEE-105: Stakeholder Obligation Compliance and Sector-Specific Risk Analysis Documents

- Policies and procedures that address stakeholder obligations and sector-specific risks.
- Sector-specific risk analysis reports that identify unique risks and compliance requirements.
- Documentation of compliance audits or assessments, including findings and actions taken to address gaps.
- Agreements or contracts with stakeholders that include compliance with sector-specific obligations and standards.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PR.AT-01.03: Cybersecurity awareness training is updated on a regular basis to reflect risks and threats identified by the organization, the organization's security policies and standards, applicable laws and regulations, and changes in individual responsibilities.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #compliance | #policy_management | #risk_management | #threat_landscape | #threat_management | #training_and_awareness

Response Guidance:

The organization's management should validate the effectiveness of cybersecurity training and update the training on a regular basis.

Provide information as to how the cybersecurity situational awareness training is updated on a regular basis to reflect risks and threats identified by the organization in its risk assessment. Provide information as to how the cybersecurity situational awareness training is updated on regular basis to reflect the organization's security policies and standards, applicable laws and regulations, and changes in individual responsibilities. Describe linkage to the operational risk and control framework. For example, management should ensure that results from social engineering testing and phishing exercises are used to shape future training initiatives that address identified weaknesses.

Examples of Effective Evidence:

EEE-007: Legal, Regulatory, and Compliance Management Documentation

- Compliance audit reports for relevant laws and regulations (e.g., GDPR, HIPAA).
- Documentation of legal advice received on cybersecurity matters, to include determinations of incident materiality.
- Records of regulatory filings and notices related to IT and cybersecurity.
- Updates to policies and procedures in response to legal and regulatory changes.
- Training records on legal and regulatory requirements for IT staff.

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.
- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

EEE-043: Cybersecurity Training, Awareness, and Expertise Access Documentation

- Agendas and materials from cybersecurity awareness events and training sessions.
- Records of accessing/retaining cybersecurity expertise and resources, including external consultants or internal experts.
- Partnerships with educational institutions or professional organizations to enhance cybersecurity knowledge.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of employee participation in external cybersecurity conferences, workshops, or courses.
- Feedback from employees on the accessibility and usefulness of cybersecurity training and expertise.

PR.AT-01.04: As new technology is deployed or undergoes change that also requires changes in practices, all impacted personnel (e.g., end-users, developers, operators, etc.) are trained on the new system and any accompanying technology and cybersecurity risks.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #emerging_technologies | #risk_management | #threat_landscape | #training_and_awareness

Response Guidance:

As new technology is deployed, the organization should be responsible for training all impacted personnel (e.g., end-users, developers, operators, etc.) on the new system and any accompanying technology and cybersecurity risks. Describe how the organization aligns their training curriculum to new or changed technology. Provide information on the organization's project change management plans that address necessary training and adoption needs.

Examples of Effective Evidence:

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.
- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

EEE-043: Cybersecurity Training, Awareness, and Expertise Access Documentation

- Agendas and materials from cybersecurity awareness events and training sessions.
- Records of accessing/retaining cybersecurity expertise and resources, including external consultants or internal experts.
- Partnerships with educational institutions or professional organizations to enhance cybersecurity knowledge.
- Records of employee participation in external cybersecurity conferences, workshops, or courses.
- Feedback from employees on the accessibility and usefulness of cybersecurity training and expertise.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

PROTECT / Awareness and Training / Specialized Role Awareness & Training

PR.AT-02.01: Mechanisms are in place to ensure that the personnel working with cybersecurity and technology (e.g., developers, DBAs, network admins, etc.) maintain current knowledge and skills related to changing threats, countermeasures, new tools, best practices, and their job responsibilities.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #staffing_and_resource_management | #threat_landscape | #threat_management | #training_and_awareness

Response Guidance:

The organization's management should establish minimum standards and certifications for personnel and require continuing specialized education to ensure expertise is maintained. Training should be current and relevant. As threats change, training should be adopted to address the changing threat landscape.

Personnel may maintain current knowledge through specific training programs, professional certifications, participation in industry groups, or other methods.

Provide information on how the organization enables employees and their managers to identify courses that they feel would be of benefit to employees to aid in terms of increasing their skills or awareness, or keeping up to speed with the latest technologies, standards, processes, or threats. Describe which metrics, reporting, and gap analysis mechanisms are in place to ensure that the personnel working with cybersecurity and technology maintain currently knowledge and skills related to changing threats, countermeasures, new tools, best practices, and their job responsibilities. As referred to GV.RR-03.01, management should have a methodology in place to measure and document technology and cybersecurity risks to determine resources required for mitigating gaps.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.
- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

EEE-043: Cybersecurity Training, Awareness, and Expertise Access Documentation

- Agendas and materials from cybersecurity awareness events and training sessions.
- Records of accessing/retaining cybersecurity expertise and resources, including external consultants or internal experts.
- Partnerships with educational institutions or professional organizations to enhance cybersecurity knowledge.
- Records of employee participation in external cybersecurity conferences, workshops, or courses.
- Feedback from employees on the accessibility and usefulness of cybersecurity training and expertise.

EEE-095: Security Training and Competency Documentation

- Security awareness and training program documentation, including topics covered, schedules, and target audiences.
- Records of participation and completion for security training sessions, workshops, and e-learning modules.
- Assessments or quizzes measuring employee understanding and retention of security concepts post-training.
- Feedback from employees on the relevance and effectiveness of security training programs.
- Continuous improvement plans for security training, based on feedback, emerging threats, and organizational changes.

PR.AT-02.02: High-risk groups, such as those with elevated privileges or in sensitive business functions (including privileged users, senior executives, cybersecurity personnel and third-party stakeholders), receive cybersecurity situational awareness training for their roles and responsibilities.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #staffing_and_resource_management | #training_and_awareness

Response Guidance:

Cybersecurity training should be aligned with the level of cybersecurity risk that exists within a business unit or high-risk group. The organization should develop a cybersecurity training program

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

that includes learning goals and objectives that align cybersecurity with employee roles and responsibilities. Privileged users, such as network, systems, or database administrators, who are granted elevated access privileges and permissions, should have additional training that focuses on the management of system's security and the judicious use of their privileged access (e.g., insider threats). Users in sensitive business functions, who are granted elevated access privileges and permissions, should also receive cybersecurity additional awareness training for their roles, and the judicious use of their privileged access (e.g., Business Email Compromise).

Describe how high-risk groups receive cybersecurity situational awareness training for their roles and responsibilities. Provide information on how situational awareness materials are made available to employees when prompted by highly visible cyber events or by regulatory alerts, and how workshops are held with senior management to provide them with situational awareness for vulnerability management and incident response.

Examples of Effective Evidence:

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.
- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

EEE-043: Cybersecurity Training, Awareness, and Expertise Access Documentation

- Agendas and materials from cybersecurity awareness events and training sessions.
- Records of accessing/retaining cybersecurity expertise and resources, including external consultants or internal experts.
- Partnerships with educational institutions or professional organizations to enhance cybersecurity knowledge.
- Records of employee participation in external cybersecurity conferences, workshops, or courses.
- Feedback from employees on the accessibility and usefulness of cybersecurity training and expertise.

EEE-071: Customer Cybersecurity Awareness Documentation

- Cybersecurity awareness materials and communications distributed to customers, such as newsletters, alerts, and guidance documents.
- Records of customer-focused cybersecurity events or webinars, including topics covered and attendee feedback.
- Documentation of customer portals or platforms that provide security tips, alerts, and updates.
- Surveys or assessments measuring customer awareness and satisfaction with the organization's cybersecurity communications.
- Case studies or examples of how customer awareness initiatives have successfully mitigated security risks.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PR.AT-02.03: All personnel (employee and third party) are made aware of and are trained for their role and operational steps in response and recovery plans.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #disaster_recovery | #incident_management | #staffing_and_resource_management | #training_and_awareness

Response Guidance:

Roles and responsibilities must be clearly described in the incident response plan and communicated to all appropriate staff in order to maintain an organized and effective incident response process. The organization may use tabletop exercises or other testing to ensure personnel know their roles and responsibilities when an incident occurs. Describe how the organization's personnel know their roles and responsibilities and the operational steps when a response is needed. Describe the roles and responsibilities within the response process.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

EEE-043: Cybersecurity Training, Awareness, and Expertise Access Documentation

- Agendas and materials from cybersecurity awareness events and training sessions.
- Records of accessing/retaining cybersecurity expertise and resources, including external consultants or internal experts.
- Partnerships with educational institutions or professional organizations to enhance cybersecurity knowledge.
- Records of employee participation in external cybersecurity conferences, workshops, or courses.
- Feedback from employees on the accessibility and usefulness of cybersecurity training and expertise.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

PR.AT-02.04: The organization maintains and enhances the skills and knowledge of the in-house staff performing incident management and forensic investigation activities.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #forensics | #incident_management | #staffing_and_resource_management | #training_and_awareness

Response Guidance:

Cybersecurity training programs should be developed and matured upon for key positions that the success of the program depends upon. Describe how training programs enhance the skills and knowledge required for the defined roles and responsibilities within incident management and forensic investigation. Provide information that supports the training topics of incident management and forensic investigation activities.

Training programs that enhance the skills and knowledge of in-house incident management staff allows an organization to retain and maintain an organized and effective incident response process. Provide information on how the organization enables employees and their managers to identify courses that they feel would be of benefit to employees to aid in terms of increasing their incident management and forensic investigation skills. Describe which metrics and reporting mechanisms are

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

in place to verify that in-house staff are maintaining and enhancing their skills and knowledge of incident management and forensic investigation activities.

Examples of Effective Evidence:

EEE-028: Investigation and Forensic Documentation

- Standard operating procedures (SOPs) for conducting security investigations and handling forensic data.
- Chain of custody forms and logs that track the handling and analysis of forensic evidence.
- Forensic toolkits and software licenses used for data analysis during investigations.
- Forensic investigation reports detailing the rigor of methods applied.
- Training certifications and other qualifications for personnel or third parties involved in forensic investigations.
- Reports from completed investigations, including methodologies, findings, and recommendations.

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.
- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

EEE-043: Cybersecurity Training, Awareness, and Expertise Access Documentation

- Agendas and materials from cybersecurity awareness events and training sessions.
- Records of accessing/retaining cybersecurity expertise and resources, including external consultants or internal experts.
- Partnerships with educational institutions or professional organizations to enhance cybersecurity knowledge.
- Records of employee participation in external cybersecurity conferences, workshops, or courses.
- Feedback from employees on the accessibility and usefulness of cybersecurity training and expertise.

PR.AT-02.05: All third party staff receive cybersecurity awareness and job training sufficient for them to perform their duties and maintain organizational security.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #staffing_and_resource_management | #training_and_awareness

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

The organization should develop a cybersecurity training program that includes learning goals and objectives that align cybersecurity with third party roles and responsibilities. The training program should consider the evolving and persistent threats and should include annual certification that third party staff understand their responsibilities to perform their duties. If the organization does not provide training to the third party staff, provide information on how the organization assesses courses and trainings at third party suppliers. Describe how the organization implements contracts and agreements with a third party for required courses and materials.

Third party staff should be required to receive situational awareness and job training that is relevant to third party personnel upon onboarding and defined frequent schedule. The situational awareness training should be updated frequently to address new technologies, threats, and risk profile. Describe how the organization ensures third party trainings are updated frequently. Provide information on the content of situational awareness materials and training to ensure it employs third party staff to maintain organizational security.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.
- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

EEE-043: Cybersecurity Training, Awareness, and Expertise Access Documentation

- Agendas and materials from cybersecurity awareness events and training sessions.
- Records of accessing/retaining cybersecurity expertise and resources, including external consultants or internal experts.
- Partnerships with educational institutions or professional organizations to enhance cybersecurity knowledge.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of employee participation in external cybersecurity conferences, workshops, or courses.
- Feedback from employees on the accessibility and usefulness of cybersecurity training and expertise.

PR.AT-02.06: The organization has established and maintains a cybersecurity awareness program through which the organization's customers are kept aware of new threats and vulnerabilities, basic cybersecurity hygiene practices, and their role in cybersecurity, as appropriate.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #policy_management | #threat_management | #training_and_awareness | #vulnerability_management

Response Guidance:

The organization should inform and update customers of current cyber threats and ongoing cybersecurity risks. There are many ways to inform customers and stakeholders of cybersecurity risks including the organization's website (e.g., security requirements that customers should follow), email, or social media, etc.

Provide information on how the organization has established and maintains a cybersecurity situational awareness program through which the organization's customers are kept aware of new threats and vulnerabilities, basic cybersecurity hygiene practices, and their role in cybersecurity, as appropriate. Describe how customer facing cybersecurity situational awareness materials are posted on the organization's public website.

Examples of Effective Evidence:

EEE-043: Cybersecurity Training, Awareness, and Expertise Access Documentation

- Agendas and materials from cybersecurity awareness events and training sessions.
- Records of accessing/retaining cybersecurity expertise and resources, including external consultants or internal experts.
- Partnerships with educational institutions or professional organizations to enhance cybersecurity knowledge.
- Records of employee participation in external cybersecurity conferences, workshops, or courses.
- Feedback from employees on the accessibility and usefulness of cybersecurity training and expertise.

EEE-071: Customer Cybersecurity Awareness Documentation

- Cybersecurity awareness materials and communications distributed to customers, such as newsletters, alerts, and guidance documents.
- Records of customer-focused cybersecurity events or webinars, including topics covered and attendee feedback.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of customer portals or platforms that provide security tips, alerts, and updates.
- Surveys or assessments measuring customer awareness and satisfaction with the organization's cybersecurity communications.
- Case studies or examples of how customer awareness initiatives have successfully mitigated security risks.

PR.AT-02.07: The organization's governing body (e.g., the Board or one of its committees) and senior management receive cybersecurity situational awareness training to include appropriate skills and knowledge to:

(1) Evaluate and manage cyber risks;

(2) Promote a culture that recognizes that staff at all levels have important responsibilities in ensuring the organization's cyber resilience; and

(3) Lead by example.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #risk_oversight | #staffing_and_resource_management | #training_and_awareness

Response Guidance:

The organization’s governing body and senior management should be included in the cybersecurity training plan and should receive training to understand the potential cyber risk of implementing business decisions as a part of their duties. The Board or one of its committees should understand cybersecurity risks and possess appropriate skills and expertise to be actively engaged in discussions on cyber risks.

Provide information on how the organization’s governing body and senior management receive cybersecurity situational awareness training which includes appropriate skills and knowledge, as required. Provide details of the various levels of cybersecurity training available based upon organizational executive role. For example, training for the organization’s governing body or senior management might include CEO fraud, whale or spear phishing, business email compromise (BEC), and other cyber threats.

Examples of Effective Evidence:

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-040: Cybersecurity Awareness and Training Program Documentation

- Plan detailing awareness initiatives and training programs, including schedules and topics.
- Records of executed awareness campaigns (e.g., phishing simulations) and training sessions.
- Engagement metrics, feedback summaries, and post-training testing used to assess program effectiveness.
- Records of follow-up remediation actions for employees that fail post-training testing.
- List of employee certifications and completion certificates for cybersecurity training.
- Improvement reports based on program feedback and metrics.

EEE-043: Cybersecurity Training, Awareness, and Expertise Access Documentation

- Agendas and materials from cybersecurity awareness events and training sessions.
- Records of accessing/retaining cybersecurity expertise and resources, including external consultants or internal experts.
- Partnerships with educational institutions or professional organizations to enhance cybersecurity knowledge.
- Records of employee participation in external cybersecurity conferences, workshops, or courses.
- Feedback from employees on the accessibility and usefulness of cybersecurity training and expertise.

EEE-072: Cybersecurity Training for Leadership Documentation

- Agendas and materials from cybersecurity training sessions specifically designed for the organization's governing body and senior management.
- Records of attendance and participation in cybersecurity training by board members and senior executives.
- Evaluations or assessments of cybersecurity knowledge before and after training sessions.
- Documentation of cybersecurity briefings or updates provided to the governing body and senior management on a regular basis.
- Feedback from senior leaders on the relevance and effectiveness of the cybersecurity training they received.

EEE-073: Governance Access to Cybersecurity Expertise Documents

- Contracts or agreements with external cybersecurity experts or advisory firms engaged to support governance activities.
- Records of cybersecurity expert consultations or briefings provided to the governing body or committees.
- Documentation of in-house cybersecurity expertise available to the governing body, including staff qualifications and roles.
- Minutes from governance meetings where cybersecurity experts provided input or guidance on decision-making.
- Evaluations of the cybersecurity expertise utilized by the governing body, assessing its impact on governance decisions.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PR.AT-02.08: Where the organization's governing authority (e.g., the Board or one of its committees) does not have adequate cybersecurity expertise, they should have direct access to the senior officer responsible for cybersecurity and independent sources of expertise to discuss cybersecurity related matters.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #organizational_structure | #risk_oversight | #training_and_awareness

Response Guidance:

The Board or one of its committees should understand cybersecurity risks and possess appropriate skills and expertise to be actively engaged in discussions on cyber risks.

Provide details on how the organization's governing authority has direct access to the senior officer responsible for cybersecurity (e.g., CISO) and independent sources of expertise to discuss cybersecurity related matters. Provide information on operational risk management framework and Board or Board related committee meetings where cybersecurity is addressed.

Examples of Effective Evidence:

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-031: Cybersecurity and Technology Officer Leadership Documentation

- Job descriptions and role profiles for the Cybersecurity Officer and Technology Officer, outlining responsibilities and qualifications.
- Strategic plans and objectives developed by the Cybersecurity Officer and Technology Officer, with documented board or executive approval.
- Records of security initiatives led by these officers, including project plans, status updates, and outcomes.
- Documentation of regular updates or briefings provided to the board and senior management by these officers.
- Evidence of the performance of 360-degree reviews of the Cybersecurity Officer and Technology Officer.
- Performance evaluations or reviews of the Cybersecurity Officer and Technology Officer, assessing their effectiveness and impact.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-043: Cybersecurity Training, Awareness, and Expertise Access Documentation

- Agendas and materials from cybersecurity awareness events and training sessions.
- Records of accessing/retaining cybersecurity expertise and resources, including external consultants or internal experts.
- Partnerships with educational institutions or professional organizations to enhance cybersecurity knowledge.
- Records of employee participation in external cybersecurity conferences, workshops, or courses.
- Feedback from employees on the accessibility and usefulness of cybersecurity training and expertise.

EEE-072: Cybersecurity Training for Leadership Documentation

- Agendas and materials from cybersecurity training sessions specifically designed for the organization's governing body and senior management.
- Records of attendance and participation in cybersecurity training by board members and senior executives.
- Evaluations or assessments of cybersecurity knowledge before and after training sessions.
- Documentation of cybersecurity briefings or updates provided to the governing body and senior management on a regular basis.
- Feedback from senior leaders on the relevance and effectiveness of the cybersecurity training they received.

EEE-073: Governance Access to Cybersecurity Expertise Documents

- Contracts or agreements with external cybersecurity experts or advisory firms engaged to support governance activities.
- Records of cybersecurity expert consultations or briefings provided to the governing body or committees.
- Documentation of in-house cybersecurity expertise available to the governing body, including staff qualifications and roles.
- Minutes from governance meetings where cybersecurity experts provided input or guidance on decision-making.
- Evaluations of the cybersecurity expertise utilized by the governing body, assessing its impact on governance decisions.

PROTECT / Data Security / Protection of Data at Rest

PR.DS-01.01: Data-at-rest is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy (e.g., through the use of encryption, authentication, access control, segregation, masking, tokenization, and file integrity monitoring).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authentication | #authorization | #critical_infrastructure | #data_classification | #data_integrity | #data_protection | #encryption | #identity_and_access_management

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

| #obfuscation | #policy_management | #security_logging_monitoring_and_alerting | #separation_of_duties

Response Guidance:

Data-at-rest is generally resident data stored on mobile devices, desktops, servers, within application and log files, databases, or storage repositories. Management is responsible for identifying where data resides, including data hosted by external service providers, and for determining whether encryption or other methods (e.g, sandboxing, authentication, access control, segregation, masking, tokenization, and file integrity monitoring) are necessary to protect data from unauthorized access or theft.

Protection should ensure that data is unreadable at rest (e.g., through encryption). Encrypting passwords in storage and transmission can be achieved by various tools, methods or software specifically designed to protect the confidentiality of passwords. Encrypting data-in-transit communications containing passwords or transmitting cryptographic password hashes instead of plaintext passwords helps protect against threats to capture passwords.

Provide information supporting how data-at-rest is protected based upon the criticality and sensitivity of the information in alignment with the data classification and protection policy. Describe the policies, standards, and controls in place for data at rest, including appropriate encryption, authentication, and access control, among others. When used, encryption algorithms must be recognized industry-wide and key management procedures must be in line with protection objectives.

Examples of Effective Evidence:

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.
- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

PR.DS-01.02: The organization implements data loss identification and prevention tools to monitor and protect against confidential data theft or destruction by an employee or an external actor.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #authentication | #authorization | #data_loss_prevention | #insider_threat | #security_logging_monitoring_and_alerting

Response Guidance:

The organization should adopt policies and implement technical controls to stop the loss and disclosure of sensitive information to outside attackers as well as inadvertent and malicious insiders. The organization should invest in tools to protect their confidential information and intellectual property by trying to prevent data leakage or data loss. Tools may include: software for blocking or encrypting files and emails with sensitive member data; disabling of USB drives; CD-ROM read, write and execute abilities; etc.

Describe the implementation of data loss identification and prevention tools used to monitor and protect against confidential data theft or destruction by an employee or an external actor. Provide information on the tools themselves and how those tools are used.

Examples of Effective Evidence:

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PR.DS-01.03: The organization defines and implements controls for the protection and use of removable media (e.g., access/use restrictions, encryption, malware scanning, data loss prevention, etc.)

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #data_loss_prevention | #infrastructure_security | #malware_protection

Response Guidance:

Removable media devices (USB, CD, and DVD) should be restricted for use, and monitored for inappropriate activity. For example, technology should be implemented to prevent users from attaching a USB drive to their portable or desktop system.

Describe how the organization defines and implements controls for the protection and use of removable media and mobile devices. Describe the organization's access control procedures for approval on enabling access to removable media. Describe how removable media and mobile device use is restricted according to the organizations policies, procedures or controls for removable storage and restricted access. Provide information on the tools and processes utilized.

Examples of Effective Evidence:

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.
- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

EEE-075: Malware and Mobile Code Defense Strategy Documents

- Policies and procedures for defending against malware and malicious mobile code, including prevention, detection, and response strategies.
- Configuration records for anti-malware tools and systems, showing protective measures in place.
- Logs and reports from anti-malware solutions, documenting detections and actions taken.
- Post-incident analysis documents that evaluate the response to malware incidents and the effectiveness of defense mechanisms.

EEE-109: Email Protection Mechanism Documents

- Policies and procedures for securing email communications, including spam filters, phishing detection, and encryption.
- Configuration records for email protection systems, demonstrating the implementation of security measures.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Training records for employees on recognizing and reporting suspicious emails and following email security best practices.
- Incident logs related to email security threats, including actions taken and resolutions.
- Audit or review reports assessing the effectiveness of email protection mechanisms and identifying areas for improvement.

PROTECT / Data Security / Protection of Data in Transit

PR.DS-02.01: Data-in-transit is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy (e.g., through the use of encryption, authentication, access control, masking, tokenization, and alternate transit paths).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authentication | #authorization | #critical_infrastructure | #data_classification | #data_integrity | #data_protection | #encryption | #identity_and_access_management | #obfuscation | #policy_management | #security_logging_monitoring_and_alerting

Response Guidance:

Data-in-transit includes two primary categories – data that is moving across public or "untrusted" networks such as the Internet, and data that is moving within the confines of private networks such as corporate Local Area Networks (LANs).

Provide information on how data-in-transit is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy. Provide information in support of controls for data-in-transit including, but not restricted to, appropriate encryption, authentication, and access control. Provide information on other methods used to protect data-in-transit (e.g., masking, tokenization, alternate transit paths, etc.) Provide detail regarding the framework and controls as it pertains to data in transit. When used, encryption algorithms must be recognized industry-wide and key management procedures must be in line with protection objectives.

Examples of Effective Evidence:

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.
- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

PROTECT / Data Security / Protection of Data in Use

PR.DS-10.01: Data-in-use is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy (e.g., through the use of encryption, authentication, access control, masking, tokenization, visual shielding, memory integrity monitoring, etc.)

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authentication | #authorization | #critical_infrastructure | #data_classification | #data_integrity | #data_protection | #encryption | #identity_and_access_management | #obfuscation | #policy_management | #security_logging_monitoring_and_alerting

Response Guidance:

Data-in-use is data that is actively being accessed and processed by a user. Authentication protections, least privilege access, and role-based access controls should be in place to combat unauthorized use and/or compromise. Describe safeguards (e.g., encryption, authentication, access control, masking, tokenization, visual shielding, memory integrity monitoring) implemented for data loss prevention.

Provide information on how data-in-use is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy. Provide

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

information on the related policies and standards. When used, encryption algorithms must be recognized industry-wide and key management procedures must be in line with protection objectives.

Examples of Effective Evidence:

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.
- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

PROTECT / Data Security / Data Backup

PR.DS-11.01: The organization defines and implements standards and procedures for configuring and performing backups and data replications, including defining backup requirements by data/application/infrastructure criticality, segregating (e.g., air-gapping) and securing backups, verifying backup integrity, and performing backup restoration testing.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #asset_management | #critical_infrastructure | #data_backup | #data_integrity | #disaster_recovery | #policy_management | #resilience

Response Guidance:

A formal backup and recovery plan describes how critical systems are backed up and restored in the event of loss or corruption of production data. Backup and recovery methods and procedures must be consistent with defined data and system recovery time objectives, recovery point objective, and impact tolerance requirements. The organization's management should reassess backup and recovery strategies as the technology and threat environments evolve. Additionally, business units should evaluate the usability and integrity of the recovered data.

Describe how the organization defines and implements standards and procedures for configuring and performing backups of information and data replications. Describe how the organization periodically conducts tests of backups to business assets (including full system recovery) to support cyber resilience. Describe any backup safeguard strategies and measures in place to mitigate ransomware attacks (e.g., air-gapping). Describe how the organization defines backup requirements by data/application/infrastructure criticality, segregating and securing backups, and verifying backup integrity. Provide information on how assets are classified and risk assessed in support of backup and testing strategy.

Examples of Effective Evidence:

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

PROTECT / Platform Security / Configuration Management

PR.PS-01.01: The organization establishes and maintains standard system security configuration baselines, informed by industry standards and hardening guidelines, to facilitate the consistent application of security settings, configurations, and versions.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #application_security | #asset_management | #patch_management | #security_baselines | #system_hardening | #vulnerability_management

Response Guidance:

The organization should develop baseline security configuration standards for production systems based on risk and in accordance with applicable configuration guidelines. A baseline configuration represents an approved set of specifications for a system, or configuration item(s) within a system, such as enabled or disabled functions or security parameters (e.g., access or password characteristics).

Provide information on how the organization establishes baseline system security configuration standards, factoring in vendor recommendations, industry standards, and hardening guidelines. Describe how the baseline security configuration standards facilitate consistent application of security settings to designated information assets. Describe how the organization determines the platforms (e.g., hardware, devices, software, operating systems, etc.) for which configuration standards will be developed. Describe the frequency and review and update of configuration standards for various platforms.

Examples of Effective Evidence:

EEE-038: Configuration Management Documentation

- Policy, standard, and/or procedure documents covering configuration management practices.
- Best practice standards used to inform configuration standards, to include evidence of adherence to hardening and least functionality objectives.
- System configuration baseline documentation and reports showing compliance with established standards.
- Change control records documenting the approval and implementation of standard system configurations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Dashboards or tools used to monitor version levels and system configurations across the organization.
- Dashboards or tools used to monitor for non-standard configurations, unsupported systems, or configuration drift.
- Audit or review findings related to configuration management with actions taken in response to findings.

PR.PS-01.02: The organization's systems are configured to provide only essential capabilities to implement the principle of least functionality.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authorization | #least_privileged_access | #separation_of_duties

Response Guidance:

The principle of least functionality provides that information systems are configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, such as ports, protocols, and/or services that are not integral to the operation of that information system. The organization should securely configure network components operating systems, applications, databases, etc., to ensure that only approved ports, protocols, and services are allowed and disable all unnecessary services, ports, and protocols.

Describe how the organization's systems are configured to provide only essential capabilities to implement the principle of least functionality. Document the security configuration standards for operating systems and components. Provide information on the process used.

Examples of Effective Evidence:

EEE-038: Configuration Management Documentation

- Policy, standard, and/or procedure documents covering configuration management practices.
- Best practice standards used to inform configuration standards, to include evidence of adherence to hardening and least functionality objectives.
- System configuration baseline documentation and reports showing compliance with established standards.
- Change control records documenting the approval and implementation of standard system configurations.
- Dashboards or tools used to monitor version levels and system configurations across the organization.
- Dashboards or tools used to monitor for non-standard configurations, unsupported systems, or configuration drift.
- Audit or review findings related to configuration management with actions taken in response to findings.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PR.PS-01.03: The organization employs detection measures and performs regular enforcement checks to ensure that non-compliance with baseline security standards is promptly identified and rectified.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #security_baselines | #security_logging_monitoring_and_alerting | #system_hardening | #vulnerability_management

Response Guidance:

Describe how the organization employs detection measures and performs regular enforcement checks to ensure that non-compliance with baseline system security standards are promptly identified and rectified, in accordance with their risk. Provide information on the detection measures, tools used and frequency of enforcement checks. Describe how criticality and risk is considered for remediation of identified risks.

Examples of Effective Evidence:

EEE-036: Vulnerability Scanning and Patch Management Documentation

- Policy, standard, and/or procedure documents covering the identification, assessment, reporting, and remediation of software and device vulnerabilities, including regular patching protocols.
- Schedules and records of patch deployment activities, including system reboots, post-patch testing, dates, systems affected, and patching outcomes.
- Documentation of patching or upgrades to standard system configuration baselines.
- Reports from vulnerability scans or assessments that inform the patch management process.
- Incident reports related to vulnerabilities that were mitigated through patch management.
- Documentation and reporting of vulnerability mitigation targets.
- Records of exceptions to, assessments of, and approvals for cases where vulnerability mitigation targets or standards are not met.
- Records demonstrating the integration of patch management and change management practices.
- Approval and review documentation for patching protocols, including impact assessments and authorization records.
- Dashboards or tools used to monitor patch levels and patch application across the target environment.
- Post-implementation reviews and post-change evaluation reports assessing the impact and success of patches and any unintended consequences.
- Audit or review findings related to vulnerability management and patching practices with actions taken in response to findings.

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.
- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

EEE-048: Exception Management and Vulnerability Handling Documentation

- Policies and procedures for handling exceptions to standard security policies, including the process for requesting and approving exceptions.
- Documentation of approved policy exceptions, including justification, risk assessment, and compensating controls.
- Vulnerability exception records that detail the rationale for not remediating certain vulnerabilities and the associated risk acceptance.
- Audit reports that review the management of policy and vulnerability exceptions.

PR.PS-01.04: The organization documents its requirements for accurate and resilient time services (e.g., synchronization to a mandated or appropriate authoritative time source) and adopts best practice guidance in implementing and using these services for logging, event correlation, forensic analysis, authentication, transactional processing, and other purposes.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authentication | #resilience | #security_baselines | #security_logging_monitoring_and_alerting

Response Guidance:

Financial institutions require their systems to maintain accurate time values for a variety of purposes. Some of these uses include the proper recording and sequencing of financial transactions; accurately recording events in audit logs to support problem resolution and forensic investigations; the time-based synchronization used by certain authentication protocols; and managing the expiry of encryption certificates and software licenses.

The resilience of the design and implementation of the organization's time services infrastructure, and the monitoring of service integrity, are of utmost importance to both the organization and its financial services and critical infrastructure partners. Loss of time integrity can create significant cascading impacts across a variety of infrastructure and application services, both within the organization and across trading partners.

The individual system clocks used to record time values in event logs, database fields, transaction records, etc. must be reliably synchronized to a known, accurately maintained time, most commonly, Coordinated Universal Time (UTC). Organizations should document their requirements for time accuracy and synchronization, to include business-related requirements (e.g., the recording of time stamps for financial transactions); technical availability, capacity, scalability, and redundancy needs; and security considerations for network components, authentication, and protocols. Organizations

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

may also want to consider the need for time synchronization/alignment with external and cloud-based services.

A variety of best-practice guidance is available for designing, implementing, securing, and managing time synchronization infrastructure components and services. Of particular relevance to CRI Profile users, NISTIR 8323r1 /1 provides guidance for the design, operation, and security of time synchronization services organized within the context of the NIST Cyber Security Framework (CSF). The CISA document "Time Guidance for Network Operators, Chief Information Officers, and Chief Information Security Officers" also provides substantive guidance and self-assessment questions.

/1 NIST Interagency/Internal Report (NISTIR) 8323r1, Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services

---

Examples of Effective Evidence:

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-050: Control Assessment and Testing Documentation

- Schedules and plans for regular assessments and testing of security controls to ensure they are functioning as intended.
- Results and reports from control assessments, including identified deficiencies and corrective actions taken.
- Documentation of testing methodologies and criteria used to evaluate the effectiveness of controls.
- Records of updates or changes to controls based on assessment findings.

PR.PS-01.05: Acceptable encryption standards, methods, and management practices are established in accordance with defined industry standards.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #compliance | #data_protection | #encryption | #industry_standards | #obfuscation | #policy_management

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

The organization should establish encryption standards, methods, and management practices in accordance with defined industry standards. Responses should include evidence that the encryption standards, methods, and management practices are built upon these industry standards. Encryption algorithms must be recognized industry-wide and key management procedures must be in line with protection objectives. Provide information on the related standards, methods, and management practices.

Examples of Effective Evidence:

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.
- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

PR.PS-01.06: The organization employs defined encryption methods and management practices commensurate with the criticality of the information being protected and the inherent risk of the technical environment where used.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #data_classification | #data_protection | #encryption | #obfuscation | #policy_management | #risk_management

Response Guidance:

Data-at-rest, data-in-use, and data-in-transit should employ encryption methods and management practices to protect the confidentiality and integrity of data. Describe how the organization implements encryption methods and management practices commensurate with the criticality of the information being protected and the inherent risk of the technical environment where used.

Responses should utilize a cryptography and key management standard or policy that is aligned to the cyber risk management program to identify inherent risk, and criticality of the information being protected to determine whether encryption is necessary to protect data from unauthorized access or theft. When used, encryption algorithms must be recognized industry wide and key management procedures must be in line with protection objectives.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.
- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

PR.PS-01.07: Cryptographic keys and certificates are tracked, managed, and protected throughout their lifecycles, to include for compromise and revocation.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #cryptography_management

Response Guidance:

Describe how the organization tracks, manages, and protects cryptographic keys and certificates throughout their lifecycle (e.g., from generation to destruction) while maintaining operational availability. Provide information of how an organization securely manages keys and certificates used for third party connections and within third party (e.g., Cloud) environments. For example, cryptography public and private keys that are distributed between sender and receiver should utilize a secure TLS or SSL connection to prevent compromise. Responses should provide information on established cryptography and key management standards implemented to ensure keys and certificates are securely managed to maintain confidentiality and integrity of an organization's sensitive information.

Key revocation should be included within the cryptography key lifecycle to deactivate a public key certificate or symmetric encryption key that is compromised or no longer needed. Describe key revocation processes and procedures. Responses should include evidence of an organization enforcing cryptography standards and policies.

Examples of Effective Evidence:

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

PR.PS-01.08: End-user mobile or personal computing devices accessing the organization's network employ mechanisms to protect network, application, and data integrity, such as "Mobile Device Management (MDM)" and "Mobile Application Management (MAM)" technologies, device fingerprinting, storage containerization and encryption, integrity scanning, automated patch application, remote wipe, and data leakage protections.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #application_security | #data_protection | #encryption | #infrastructure_security | #mobile_device_management | #patch_management | #security_baselines | #security_logging_monitoring_and_alerting | #system_integrity | #vulnerability_management

Response Guidance:

Organizations should establish and maintain an up-to-date inventory that is inclusive of external information systems (e.g., end-user mobile or personal computing devices). Processes should be in place to review inventories to ensure all devices accessing the organization's network are approved or removed if unauthorized.

Provide information on how end-user mobile and/or personal computing devices accessing the organization's network employ mechanisms designed to protect network, application, and data integrity. Provide information on policies and procedures that are established for end-user mobile or personal computing devices designed to keep corporate data secure. Responses can provide evidence of "Mobile Device Management (MDM)" and "Mobile Application Management (MAM)" technologies, device fingerprinting, storage containerization and encryption, integrity scanning, automated patch application, remote wipe when a personal device is lost or stolen, and data leakage protections (e.g., end-user training).

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of user account creation, modification, and termination processes.

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.
- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

PR.PS-01.09: Endpoint systems implemented using virtualization technologies employ mechanisms to protect network, application, and data integrity, such as restricting access to local network and peripheral devices, multi-factor authentication, locking-down device source network locations, and data leakage protections.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #application_security | #authentication | #authorization | #endpoint_security | #infrastructure_security | #multi_factor_authentication | #security_baselines | #security_logging_monitoring_and_alerting

Response Guidance:

Virtualization technologies or virtual machines (VMs) allow for users to run and access a virtual instance of guest operating system independent from the underlying hardware. A hypervisor is a software utilized to host a VM and allow the system's resources to be isolated for a single user. Although running hypervisors can limit the impact of a compromise compared to a host operating system, it is still crucial that mechanisms are in place to protect network, application, and data integrity. Organizations should also keep software up-to-date

Responses include mechanisms employed such as restricting access to local network and peripheral devices, multi-factor authentication, locking-down service network locations, and data leakage protections. Provide information on mechanisms that are implemented on endpoint systems using virtualization technologies to protect network, application, and data integrity.

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.
- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

PROTECT / Platform Security / Software Maintenance & Replacement

PR.PS-02.01: The organization defines and implements controls to identify patches to technology assets, assess patch criticality and risk, test patches, and apply patches within risk/criticality-based target time frames.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #application_security | #asset_management | #patch_management | #vulnerability_management

Response Guidance:

Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. Patch management is required by various security compliance frameworks, mandates, and other policies. For example, NIST Special Publication (SP) 800-532 requires the SI-2, Flaw Remediation security control, which includes installing security-relevant software and firmware patches, testing patches before installing them, and incorporating patches into the organization's configuration management processes. Similarly, ISO 27001 A.12.6.1, Management of Technical Vulnerabilities, requires the timely implementation of patches for newly discovered technical vulnerabilities to ensure the organization maintains acceptable risk levels. Another example PCI-DSS, which requires that the latest patches be installed and sets a maximum timeframe for installing the most critical patches.

Effective patch management may include establishing procedures to stay abreast of patches, to test availability in a segregated environment, and to install them when appropriate.

Describe the implemented controls used to identify patches to technology assets, assess patch criticality, and risk, and test and apply the patch within risk/criticality-based target time frames. Provide information on related tools and frequency.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-036: Vulnerability Scanning and Patch Management Documentation

- Policy, standard, and/or procedure documents covering the identification, assessment, reporting, and remediation of software and device vulnerabilities, including regular patching protocols.
- Schedules and records of patch deployment activities, including system reboots, post-patch testing, dates, systems affected, and patching outcomes.
- Documentation of patching or upgrades to standard system configuration baselines.
- Reports from vulnerability scans or assessments that inform the patch management process.
- Incident reports related to vulnerabilities that were mitigated through patch management.
- Documentation and reporting of vulnerability mitigation targets.
- Records of exceptions to, assessments of, and approvals for cases where vulnerability mitigation targets or standards are not met.
- Records demonstrating the integration of patch management and change management practices.
- Approval and review documentation for patching protocols, including impact assessments and authorization records.
- Dashboards or tools used to monitor patch levels and patch application across the target environment.
- Post-implementation reviews and post-change evaluation reports assessing the impact and success of patches and any unintended consequences.
- Audit or review findings related to vulnerability management and patching practices with actions taken in response to findings.

PR.PS-02.02: The organization establishes standards and practices for ongoing application management to ensure that applications remain secure and continue to meet organizational needs.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #application_security | #application_security_testing | #policy_management | #vulnerability_management

Response Guidance:

Provide information on how the organization ensures that applications remain secure and continue to meet organizational needs. For example, automated patch management processes being employed on a frequent basis for applications.

An organization should establish standards and practices for ongoing application management. Provide evidence of standards and procedures being in place. Standards and procedures should cover application security testing, secure coding practices, and application design. Describe the process for secure system development including supporting infrastructure and any “off-the-shelf” applications. Provide information supporting secure System Development Life Cycle (SDLC) for in-house software design and development. Documented standards and procedures should be reviewed and updated at least annually. Describe processes for end-users to request application

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

changes and new functionality. Describe the policies and practices used to address unsupported and end-of-life applications.

Examples of Effective Evidence:

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

PR.PS-02.03: Technology obsolescence, unsupported systems, and end-of-life decommissioning/replacements are addressed in a risk-based manner and actively planned for, funded, managed, and securely executed.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #asset_management | #vulnerability_management

Response Guidance:

Responses provide System Development Lifecycle standards and processes that describe how the organization plans for technology obsolescence, unsupported systems, and end-of-life decommissioning/replacements. Describe how the organization considers new technology advancement and integration of new systems in a risk-based manner to actively plan, fund, manage, and securely execute end-of-life decommissioning/replacements.

Examples of Effective Evidence:

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PROTECT / Platform Security / Hardware Maintenance

PR.PS-03.01: The organization defines and implements controls for the on-site and remote maintenance and repair of the organization's technology assets (e.g., work must be performed by authorized personnel, use of approved procedures and tools, use of original or vendor-approved spare parts).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #authentication | #authorization | #identity_and_access_management | #infrastructure_security | #physical_security | #policy_management | #privileged_access | #remote_access

Response Guidance:

Describe the procedures, tools, and controls in place for the maintenance and repair of the organization's technology assets, including but not limited to off-premise assets such as cloud computing. Changes to assets should be formally documented within the change management process. Describe how physical entry controls, employee observation, equipment maintenance, removal of assets, and related controls are in place.

Describe how the remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access or tampering. Describe the supporting processes and tools that are in place along with roles and responsibilities.

Examples of Effective Evidence:

EEE-077: Physical and Environmental Security Documents

- Documentation of environmental controls (e.g., fire suppression, climate control) and physical security measures (e.g., access controls, surveillance systems).
- Maintenance and inspection records for environmental and physical security equipment.
- Incident logs related to environmental hazards or physical security breaches, including responses and outcomes.
- Security audit reports evaluating the adequacy of environmental and physical security controls.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PROTECT / Platform Security / Log Record Generation

PR.PS-04.01: The organization establishes and regularly reviews log management standards and practices, to include the types of events to be detected, log content, security and access considerations, monitoring protocols, integrity checking mechanisms, and retention periods.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #data_retention | #security_logging_monitoring_and_alerting | #system_integrity

Response Guidance:

A log record provides the ability to show who has accessed an information system, what operations the user has performed during a given period, errors preventing an application from running, and monitor users (both authorized and unauthorized) for access, authentication, usage, connections, devices, and anomalous behavior. Organizations should have a log management standards and practices that consider potential future needs for log use in forensic investigations and as forensic evidence.

Describe how log management standards and practices have been established to include formal requirements for the types of events to be detected, explicit content to be logged, security and access considerations to prevent unauthorized access, monitoring protocols, integrity checking mechanisms, and retention periods. Provide information regarding the content and structure of logs. Describe how logs are reviewed and analyzed (e.g., input into the security operations center tool).

Examples of Effective Evidence:

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PR.PS-04.02: The organization defines the scope and coverage of audit/log records to be created and monitored (i.e., internal and external environments, devices, and applications/services/software to be monitored) and has controls in place to ensure that the intended scope is fully covered and that no logging failures are inhibiting the collection of required logs.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #security_baselines | #security_logging_monitoring_and_alerting | #system_hardening | #technology_availability

Response Guidance:

Audit/log records are created to show traceability of who has accessed an information system, what operations the user has provided during a given period, errors preventing an application from running, and monitor users (both authorized and unauthorized) for access, authentication, usage, connections, devices, and anomalous behavior. Provide information on how logging and monitoring policies, standards, and procedures are established and managed to define the scope and coverage of audit/log records. Describe the coverage of internal and external environments, devices, and applications/software to be monitored.

Describe how policies and/or controls are implemented to ensure that the intended scope is fully covered and that no logging failures are inhibiting the collection of required logs. Describe processes related to planning for logging failures (e.g., exceeding audit log storage capacity, access failures, hardware failure, etc.). Describe fail-safe logging mechanisms utilized when the primary logging capability fails related to alerting, alternate storage, shutdown of the system, etc.

Examples of Effective Evidence:

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PR.PS-04.03: The organization's activity logs and other security event logs are generated, reviewed, securely stored, and retained in accordance with data retention obligations and established standards.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #data_protection | #data_retention | #least_privileged_access | #policy_management | #security_logging_monitoring_and_alerting

Response Guidance:

All systems, including network devices should have logging enabled. The organization should maintain sufficient logs of physical and logical access to review an event. Information captured in logs is critical to detecting malicious activity and provide incident responders with crucial evidence for investigations. Logs may be modified by attackers, including insiders, to hide malicious activity. Logs should be reviewed periodically for completeness and to ensure they have not been deleted, modified, overwritten, or compromised. This is most easily accomplished by using a centralized server that maintains logs in a separate, secure location.

Describe how the organization's activity logs and other security event logs are generated, reviewed, securely stored, and retained in a secure manner and in accordance with data retention obligations and established standards. Refer to PR.PS-04.01 and PR.PS-04.02, to establish log management standards and practices and define the scope and coverage of audit/log records to be created and monitored according to the data retention obligations and established standards. Provide information on the organization's review process of the audit/log records. Provide information on the storage and length of time event logs are stored in accordance with data retention policies, procedures, and standards.

Examples of Effective Evidence:

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PROTECT / Platform Security / Unauthorized Software Installation & Execution

PR.PS-05.01: The organization has policies, procedures, and tools in place to detect and block malware from infecting networks and systems, including automatically updating malware signatures and behavior profiles on all endpoints.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #endpoint_security | #infrastructure_security | #malware_protection | #policy_management | #security_logging_monitoring_and_alerting

Response Guidance:

Malware has become more and more sophisticated in recent years, evolving from annoyance attacks or proof-of-concept attacks to rootkits and key loggers designed to steal critical business data. Anti-virus and anti-malware tools help protect data and systems by detecting malicious code or malware, such as viruses, Trojans, rootkits, and destructive malware. Having antivirus and malware protection on systems, desktops, laptops, and other devices is critical given today's threats. The organization should implement and actively manage anti-virus and anti-malware software, including regular updates based on the risk profile of the organization.

Describe the policies, procedures, and tools in place to detect and block malware from infecting networks and systems. Describe how the organization has processes to automatically update malware signatures and behavior profiles on all endpoints. Provide information on malware protection and intrusion protection. Describe process to identify devices that have not been updated within a given period of time (i.e., inaccessible).

Examples of Effective Evidence:

EEE-039: Malware Protection and Incident Detection Documentation

- Anti-malware policies and procedures, including strategies for prevention, detection, and response.
- Logs from anti-malware solutions showing coverage, detection, and remediation of malicious software.
- Exception reports and tracking of malware detection failures and gaps.
- Incident response plans that include specific protocols for handling malware-related incidents.
- Post-incident analysis reports that evaluate the effectiveness of malware protection strategies.

EEE-075: Malware and Mobile Code Defense Strategy Documents

- Policies and procedures for defending against malware and malicious mobile code, including prevention, detection, and response strategies.
- Configuration records for anti-malware tools and systems, showing protective measures in place.
- Logs and reports from anti-malware solutions, documenting detections and actions taken.
- Post-incident analysis documents that evaluate the response to malware incidents and the effectiveness of defense mechanisms.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-109: Email Protection Mechanism Documents

- Policies and procedures for securing email communications, including spam filters, phishing detection, and encryption.
- Configuration records for email protection systems, demonstrating the implementation of security measures.
- Training records for employees on recognizing and reporting suspicious emails and following email security best practices.
- Incident logs related to email security threats, including actions taken and resolutions.
- Audit or review reports assessing the effectiveness of email protection mechanisms and identifying areas for improvement.

PR.PS-05.02: The organization implements safeguards against unauthorized mobile code (e.g., JavaScript, ActiveX, VBScript, PowerShell, etc.) on mobile, end point, and server systems.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #endpoint_security | #malware_protection | #mobile_device_management | #security_baselines | #security_logging_monitoring_and_alerting

Response Guidance:

Mobile code is any program, application, or content that can be transmitted across a network and run-on a variety of platforms (e.g., JavaScript, ActiveX, VBScript, PowerShell, etc.). Mobile code usage should be limited and restricted to defined authorized uses on mobile, end point (e.g., laptops, workstations), and server systems. Policies and procedures should be in place to outline the acceptable and unacceptable uses of mobile code in systems to prevent from malware.

Provide information on how the organization monitors the use of mobile code (e.g., audit logs) to detect unauthorized use. Describe safeguards implemented (e.g., network intrusion detection systems, intrusion prevention systems to monitor network traffic) on mobile, end point, and server systems to combat unauthorized mobile code.

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-075: Malware and Mobile Code Defense Strategy Documents

- Policies and procedures for defending against malware and malicious mobile code, including prevention, detection, and response strategies.
- Configuration records for anti-malware tools and systems, showing protective measures in place.
- Logs and reports from anti-malware solutions, documenting detections and actions taken.
- Post-incident analysis documents that evaluate the response to malware incidents and the effectiveness of defense mechanisms.

PR.PS-05.03: The organization has policies, procedures, and tools in place to detect, isolate, and block the use of attached malware or malicious links present in email or message services.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #endpoint_security | #infrastructure_security | #malware_protection | #policy_management

Response Guidance:

The three major protocols used for the majority of electronic mail (POP, IMAP and SMTP) are clear text protocols that were designed without security or privacy in mind. An organization's email can be subject to interception, alteration and counterfeiting by anyone on the virtual path between the sender and the recipient. Spear phishing and whale phishing are common social engineering attacks that use fraudulent emails to acquire sensitive information or financial gain. As referenced in PR.AT-01.01, organizations should have cyber awareness trainings in place that educate personnel on secure email use, phishing attempts, and malicious links present in email or message services.

As such, the organization should implement email or message services protection mechanisms to protect the organization from malware or viruses.

Describe which policies, procedures, and tools are in place to automatically scan, detect, isolate, and block the use of attached malware or malicious links presented in email or message services. Provide information on the tools utilized.

Examples of Effective Evidence:

EEE-039: Malware Protection and Incident Detection Documentation

- Anti-malware policies and procedures, including strategies for prevention, detection, and response.
- Logs from anti-malware solutions showing coverage, detection, and remediation of malicious software.
- Exception reports and tracking of malware detection failures and gaps.
- Incident response plans that include specific protocols for handling malware-related incidents.
- Post-incident analysis reports that evaluate the effectiveness of malware protection strategies.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-075: Malware and Mobile Code Defense Strategy Documents

- Policies and procedures for defending against malware and malicious mobile code, including prevention, detection, and response strategies.
- Configuration records for anti-malware tools and systems, showing protective measures in place.
- Logs and reports from anti-malware solutions, documenting detections and actions taken.
- Post-incident analysis documents that evaluate the response to malware incidents and the effectiveness of defense mechanisms.

EEE-109: Email Protection Mechanism Documents

- Policies and procedures for securing email communications, including spam filters, phishing detection, and encryption.
- Configuration records for email protection systems, demonstrating the implementation of security measures.
- Training records for employees on recognizing and reporting suspicious emails and following email security best practices.
- Incident logs related to email security threats, including actions taken and resolutions.
- Audit or review reports assessing the effectiveness of email protection mechanisms and identifying areas for improvement.

PROTECT / Platform Security / Secure Systems Development Practices

PR.PS-06.01: The organization implements Secure Systems Development Lifecycle processes for in-house software design, configuration, and development, employing best practices from secure-by-design methodologies (e.g., secure coding, code review, application security testing, etc.) during all phases of both traditional and agile projects.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #application_security | #application_security_testing | #secure_system_development | #security_baselines | #technology_development_lifecycle | #vulnerability_management

Response Guidance:

The secure System Development Life Cycle (SDLC) is the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal. For any SDLC, information security should be integrated to ensure appropriate protection of the information that the system will transmit, process, and store. Security should be integrated during all phases of both traditional and agile projects. Secure-by-design methodologies (e.g., secure coding, code review, application security testing, etc.) should apply to both traditional and agile projects during all phases.

Describe the process for secure system development, including supporting infrastructure and any "off-the-shelf" applications. Provide information supporting secure SDLC for in-house software design, configuration, and development. Describe how the organization employs best practices from

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

secure-by-design methodologies and vendor recommendation during all phases of both traditional and agile projects.

Examples of Effective Evidence:

EEE-036: Vulnerability Scanning and Patch Management Documentation

- Policy, standard, and/or procedure documents covering the identification, assessment, reporting, and remediation of software and device vulnerabilities, including regular patching protocols.
- Schedules and records of patch deployment activities, including system reboots, post-patch testing, dates, systems affected, and patching outcomes.
- Documentation of patching or upgrades to standard system configuration baselines.
- Reports from vulnerability scans or assessments that inform the patch management process.
- Incident reports related to vulnerabilities that were mitigated through patch management.
- Documentation and reporting of vulnerability mitigation targets.
- Records of exceptions to, assessments of, and approvals for cases where vulnerability mitigation targets or standards are not met.
- Records demonstrating the integration of patch management and change management practices.
- Approval and review documentation for patching protocols, including impact assessments and authorization records.
- Dashboards or tools used to monitor patch levels and patch application across the target environment.
- Post-implementation reviews and post-change evaluation reports assessing the impact and success of patches and any unintended consequences.
- Audit or review findings related to vulnerability management and patching practices with actions taken in response to findings.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PR.PS-06.02: The architecture, design, coding, testing, and operationalization of system solutions address the unique security, resilience, technical, and operational characteristics of the target platform environment(s) (e.g., distributed system, mainframe, cloud, API, mobile, database, etc.)

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #application_security | #architecture | #cryptography_management | #infrastructure_security | #mission_and_strategy | #resilience

Response Guidance:

As mentioned in PR.PS-06.01, the secure System Development Life Cycle (SDLC) is the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal.

Provide information supporting the SDLC process addressing the unique security, resilience, technical, and operational characteristics of the target platform environment(s). Describe how software development integrates robust resilience (e.g., threat modeling, secure design principles, etc.). Testing of system solutions should be performed to validate the functionality, performance, and alignment of resilience, technical, and operating characteristics of the target platform environment(s). Different target implementation platforms and environments (e.g., distributed systems, mainframe, cloud, API, mobile, database, etc.) will have unique security best practice characteristics. Describe the secure SDLC practices that may be specific to development for each target platform or environment (e.g., based on vendor recommendations).

Examples of Effective Evidence:

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PR.PS-06.03: Functional, operational, resilience, and security requirements for system development and implementation projects are documented, agreed to by relevant stakeholders, and tracked and managed through development, testing, assurance, acceptance, and delivery.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #application_security | #architecture | #infrastructure_security | #resilience | #secure_system_development | #security_baselines | #technology_development_lifecycle

Response Guidance:

Functional, operational, resilience, and security requirements should be established and managed within the SDLC process. Provide information to support that functional, operational, resilience, and security requirements are agreed upon by relevant stakeholders. Describe how each phase of the SDLC process (e.g., development, testing, assurance, acceptance, and delivery) is tracked and managed. Describe the use of requirements traceability matrices, burn-down charts, or other tools to track and manage stakeholder requirements in the SDLC process.

Examples of Effective Evidence:

EEE-053: Project Governance, Management, and Quality Assurance Documentation

- Project governance frameworks or charters that define roles, responsibilities, and decision-making processes.
- Stakeholder analysis documents and communication plans for engaging with project stakeholders.
- Project management plans that include quality control measures, checkpoints, risk mitigation strategies, and contingency planning.
- Risk assessment templates and completed assessments for technology projects, identifying potential delivery risks.
- Quality assurance policies and procedures for overseeing project deliverables and outcomes.
- Checklists and tools used for quality control during project execution.
- Meeting minutes and action items from project steering committees, governance boards, or risk management discussions within project teams, including actions taken to address identified risks.
- Records of project audits or reviews focused on quality aspects.
- Feedback and satisfaction surveys from stakeholders regarding project outcomes and engagement.
- Reports on project performance, governance effectiveness, and risk management effectiveness, including lessons learned.
- Training documentation for project managers and team members on quality management practices and risk assessment and management techniques.
- Post-project reviews or retrospectives that analyze risk management effectiveness and lessons learned.
- Documentation of project management standards, methodologies, and best practices adopted by the organization

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

PR.PS-06.04: Systems development and testing tools, processes, and environments employ security mechanisms to protect and improve the integrity and confidentiality of both the SDLC process and the resulting product (e.g., secured code repositories, segmented environments, automated builds, etc.)

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #application_security | #application_security_testing | #architecture | #cryptography_management | #data_protection | #infrastructure_security | #secure_system_development | #security_baselines | #technology_development_lifecycle

Response Guidance:

System development and testing tools, processes, and environments should incorporate security mechanisms to protect and improve the integrity and confidentiality of both the SDLC process and the resulting product. The organization should implement security measures to protect the systems and data used during the development lifecycle. Organizations should have a separation between production and non-production environments, control identity and access management, identify vulnerabilities to be remediated, and protect data against unauthorized access. Further, the organization should follow development practices (e.g., DevSecOps) and tactics (e.g., CI/CD) to improve the SDLC processes, security, and confidentiality.

Examples of Effective Evidence:

EEE-055: Network and System Segmentation Implementation Documentation

- Written policies detailing the approach to network security and system segmentation, including criteria for segmenting resources and strategies for enhancing security.
- Network diagrams showing the segmentation of the network into different zones or segments for security purposes, including firewalls and access control lists.
- Configuration records, change logs, or documentation demonstrating the implementation of segmentation controls.
- Audit reports assessing and evaluating the effectiveness of network and system segmentation in reducing risk, isolating, and protecting critical assets.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Incident response records showing the role of network segmentation in containing security events.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

PR.PS-06.05: A software security testing and validation strategy is developed and implemented in the development lifecycle of all software projects, defining testing requirements and plans; performing/automating testing, vulnerability scanning, and migration activities; and supporting code integrity verification (e.g., using digital signatures).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #application_security_testing | #cryptography_management | #patch_management | #penetration_testing | #secure_system_development | #technology_development_lifecycle | #vulnerability_management

Response Guidance:

Newly created software may have security weaknesses; therefore, the organization should assess the cyber risks before applications are released for business use. Provide information on how the organization defines testing requirements and plans. Describe how the organization assesses the cyber risks of software prior to deployment using penetration testing and/or vulnerability scanning. Provide information on the assessment process and any tools used.

Provide information on how the security testing and validation strategy is implemented throughout the development lifecycle of all software projects. Describe how the organization develops and implements a software security testing and validation strategy. Responses should include code integrity verifications implemented in the development lifecycle for all software projects. Describe how security testing tools and procedures are adapted to the various platforms and environments in use (e.g., mainframe, mobile, etc.).

Examples of Effective Evidence:

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

PR.PS-06.06: The system development lifecycle remediates known critical vulnerabilities, and critical vulnerabilities discovered during testing, prior to production deployment.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #application_security_testing | #patch_management | #secure_system_development | #technology_development_lifecycle | #vulnerability_management

Response Guidance:

Describe how the organization has established and maintains capabilities for ongoing vulnerability management, including systematic scans as part of SDLC policies, standards, and processes. Provide information on SDLC development and deployment practices (e.g., DevSecOps) and tactics (e.g., CI/CD pipelines) that can help identify and remediate critical vulnerabilities prior to production deployment. Responses include automated security testing capabilities to identify vulnerabilities early in the software development process.

Describe how the organization performs testing to identify vulnerabilities prior to deployment. Provide information on the assessment process and any tools used. Describe how any exceptions are documented, assessed, and approved.

Examples of Effective Evidence:

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PR.PS-06.07: DevOps/DevSecOps practices and procedures are aligned with Systems Development Lifecycle, security operations, and technology service management processes.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #policy_management | #secure_system_development | #technology_development_lifecycle

Response Guidance:

The organization should adopt DevOps/DevSecOps practices and procedures, as appropriate, to ensure there is security testing incorporated during every phase of the SDLC. The organization should integrate security practices throughout the SDLC to reduce, mitigate and remediate the number of vulnerabilities prior to production deployment, and shorten the timeframe of the development lifecycle. Responses include alignment of practices, procedures, and processes for a more secure, robust Systems Development Lifecycle.

Describe how DevOps/DevSecOps practices and procedures are aligned with Systems Development Lifecycle, security operations, and technology service management processes.

Examples of Effective Evidence:

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

PR.PS-06.08: The design, configuration, security control, and operation of key applications and system services are documented sufficiently to support ongoing management, operation, change, and assessment.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #security_baselines | #system_hardening

Response Guidance:

The design, configuration, security control, and operation of key applications and system services should be clearly defined and documented. Responses include established processes for identifying and managing documentation changes throughout the SDLC. Change management operations should support system development lifecycle phases and related activities. Provide information on how plans support the ongoing management, operation, change and assessment of key applications

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

and system services. Describe the standard types of system documentation that the organization requires for all systems (e.g., system requirements) and specific to particular platforms and environments (e.g., mobile code documentation).

Examples of Effective Evidence:

EEE-087: Security Control and Process Improvement Documents

- Continuous improvement plans for security controls and processes, detailing objectives, actions, timelines, and responsible parties.
- Budget requests and justifications for improvement recommendations.
- Documentation of security control assessments, including findings and recommendations for enhancements.
- Change management records for updates to security processes and controls, including rationale and outcomes.
- Feedback collection mechanisms and reports from users and stakeholders on security controls, informing improvement plans.
- Performance metrics and monitoring reports that track the effectiveness of security controls and process improvements over time.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

PR.PS-06.09: End-user developed solutions, to include models used to support critical business processes and decisions, are formally identified and managed in alignment with their criticality and risk.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #business_impact_analysis | #critical_infrastructure | #risk_management

Response Guidance:

End-user developed solutions should be identified, managed, and tracked in alignment with their criticality and risk. Solutions should include models and documented business process flows to support critical business processes and decisions. Organizations should define the criteria for the models and end-user computing (EUC) managed, and then develop an inventory of all qualifying items. Based on the criticality and risk of the end-user developed solution, the organization should establish processes to undergo additional security testing. Critical models and business decision-support tools may require “general IT controls” (e.g, backups, structured testing, version control, etc.)

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

to be applied to satisfy audit expectations. For example, if an end-user developed solution connects to the public internet and/or support critical business processes, then penetration testing should be performed.

Describe how the organization develops models to be used to support critical business processes and decisions. Provide information on how end-user developed solutions and models are formally identified and managed in alignment with their criticality and risk.

Examples of Effective Evidence:

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

PR.PS-06.10: The organization establishes policies and procedures for the secure design, configuration, modification, and operation of databases, data stores, and data analytics platforms consistent with the criticality of the data being managed.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #architecture | #data_protection | #policy_management | #security_baselines

Response Guidance:

The organization should establish policies and procedures for the effective implementation and secure design, configuration, modification, and operation of databases, data stores, and data analytics platforms. Policies and procedures should also specifically address privileged user and automated system connections (i.e., service connections) to databases and data stores. Policies and procedures should reflect considerations of the criticality of the data being managed and potential to adversely impact the organizational operations. Provide information of established configuration management policies and procedures.

Examples of Effective Evidence:

EEE-036: Vulnerability Scanning and Patch Management Documentation

- Policy, standard, and/or procedure documents covering the identification, assessment, reporting, and remediation of software and device vulnerabilities, including regular patching protocols.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Schedules and records of patch deployment activities, including system reboots, post-patch testing, dates, systems affected, and patching outcomes.
- Documentation of patching or upgrades to standard system configuration baselines.
- Reports from vulnerability scans or assessments that inform the patch management process.
- Incident reports related to vulnerabilities that were mitigated through patch management.
- Documentation and reporting of vulnerability mitigation targets.
- Records of exceptions to, assessments of, and approvals for cases where vulnerability mitigation targets or standards are not met.
- Records demonstrating the integration of patch management and change management practices.
- Approval and review documentation for patching protocols, including impact assessments and authorization records.
- Dashboards or tools used to monitor patch levels and patch application across the target environment.
- Post-implementation reviews and post-change evaluation reports assessing the impact and success of patches and any unintended consequences.
- Audit or review findings related to vulnerability management and patching practices with actions taken in response to findings.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

PROTECT / Platform Security / Technology Operations, Service, & Support

PR.PS-07.01: The organization's technology operations, process verification, error detection, issue management, root cause analysis, and problem management functions are formally documented, monitored, and KPIs are regularly reported to stakeholders.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #incident_management | #issue_management | #lessons_learned | #metrics_and_reporting | #root_cause_analysis

Response Guidance:

Describe formally documented policies, standards, and procedures in place for technology operations, process verification, error detection, issue management, root cause analysis, and problem management functions. Common frameworks similar to ITIL and COBIT can help organizations define and manage problem management functions, and implement processes for

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

issue management. Once the organization identifies an issue, management should develop corrective actions to address. Policies, standards, and procedures should be established to document the issue, outline roles and responsibilities, and track progress until remediation. Describe tracking of status in finding remediation and how it is provided to stakeholders.

Provide information on the effectiveness of technology operations, process verification, error detection, issue management, root cause analysis, and problem management functions through KPIs. Additionally, describe information related to reporting KPIs regularly to applicable stakeholders.

Examples of Effective Evidence:

EEE-009: Audit and Remediation Documentation

- Internal audit reports on IT and cybersecurity controls.
- External audit findings and recommendations related to cybersecurity.
- Management responses and action plans addressing audit observations.
- Follow-up reports on the implementation of audit recommendations.
- Third-party assurance reports (e.g., SOC 2, ISO/IEC 27001 certifications).

EEE-050: Control Assessment and Testing Documentation

- Schedules and plans for regular assessments and testing of security controls to ensure they are functioning as intended.
- Results and reports from control assessments, including identified deficiencies and corrective actions taken.
- Documentation of testing methodologies and criteria used to evaluate the effectiveness of controls.
- Records of updates or changes to controls based on assessment findings.

EEE-054: Technology Service Performance and Support Monitoring Documentation

- Service level agreements (SLAs) and key performance indicators (KPIs) for technology services and support functions.
- Documentation for service catalogs, service support systems, or other mechanisms for end-users to request services.
- Monitoring dashboards or reports that track service performance against SLAs and KPIs.
- Records of service incidents, including response times, resolution details, and customer feedback.
- Procedures for managing and improving technology service performance.

PR.PS-07.02: Technology service and support functions address stakeholder expectations (e.g., through stated requirements, SLAs, or OLAs) and performance is monitored and regularly reported to stakeholders.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #technology_development_lifecycle

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Describe how technology service and support functions address stakeholder expectations (e.g., through stated requirements, SLAs, or OLAs). Describe how the organization develops SLAs or OLAs in agreement with stakeholder expectations. Describe how IT services are described and offered to end-users. Describe end-user service request processes, to include how requests are logged, fulfilled, and tracked to closure. Describe how business expectations for IT support services are defined, tracked, managed, and reported to stakeholders.

Develop, monitor, and report on the performance of technology service and support functions regularly to stakeholders. Provide information on how stakeholder expectations are addressed and measure the effectiveness or efficiency of technology service and support functions.

Examples of Effective Evidence:

EEE-054: Technology Service Performance and Support Monitoring Documentation

- Service level agreements (SLAs) and key performance indicators (KPIs) for technology services and support functions.
- Documentation for service catalogs, service support systems, or other mechanisms for end-users to request services.
- Monitoring dashboards or reports that track service performance against SLAs and KPIs.
- Records of service incidents, including response times, resolution details, and customer feedback.
- Procedures for managing and improving technology service performance.

PROTECT / Technology Infrastructure Resilience / Logical Access Protections

PR.IR-01.01: Networks, systems, and external connections are segmented (e.g., using firewalls, software-defined networks, guest wireless networks, etc.) to implement defense-in-depth and access isolation principles.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #architecture | #boundary_protection | #infrastructure_security | #network_diagrams | #network_segmentation

Response Guidance:

The organization should ensure networks, systems, and external connections are segmented (e.g., implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks). Segmenting is evidenced by using separate local area networks, virtual local area networks, or similar controls which can restrict or monitor network access as appropriate for the organization's risk. For example, networks with critical infrastructure should be segmented such that shell or administrative access is not available from the general desktop networks and only available via hardened jump servers.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Provide information on how the organization's networks, systems, and external connections are segmented to implement defense-in-depth and access isolation principles.

Examples of Effective Evidence:

EEE-055: Network and System Segmentation Implementation Documentation

- Written policies detailing the approach to network security and system segmentation, including criteria for segmenting resources and strategies for enhancing security.
- Network diagrams showing the segmentation of the network into different zones or segments for security purposes, including firewalls and access control lists.
- Configuration records, change logs, or documentation demonstrating the implementation of segmentation controls.
- Audit reports assessing and evaluating the effectiveness of network and system segmentation in reducing risk, isolating, and protecting critical assets.
- Incident response records showing the role of network segmentation in containing security events.

PR.IR-01.02: Network device configurations (e.g., firewall rules, ports, and protocols) are documented, reviewed and updated regularly and upon change to ensure alignment with network access, segmentation, traversal, and deny-all default requirements.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #architecture | #boundary_protection | #endpoint_security | #infrastructure_security | #network_diagrams | #network_segmentation | #security_baselines

Response Guidance:

Network device configurations (e.g., firewall rules, ports, and protocols) should be aligned to defined security baseline configurations. A methodology should be implemented to determine if the organization is failing to meet, is meeting, or is exceeding those established benchmarks.

Provide information on how network configurations are documented, formally reviewed, and agreed-upon. Describe how network device configurations are updated regularly and upon change to ensure alignment with network access, segmentation, traversal, and deny-all default requirements.

Examples of Effective Evidence:

EEE-055: Network and System Segmentation Implementation Documentation

- Written policies detailing the approach to network security and system segmentation, including criteria for segmenting resources and strategies for enhancing security.
- Network diagrams showing the segmentation of the network into different zones or segments for security purposes, including firewalls and access control lists.
- Configuration records, change logs, or documentation demonstrating the implementation of segmentation controls.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Audit reports assessing and evaluating the effectiveness of network and system segmentation in reducing risk, isolating, and protecting critical assets.
- Incident response records showing the role of network segmentation in containing security events.

PR.IR-01.03: The integrity and resilience of the organization's communications and control network services are enhanced through controls such as denial of service protections, secure name/address resolution, and/or alternate communications paths.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #infrastructure_security | #resilience | #security_logging_monitoring_and_alerting

Response Guidance:

An organization's network perimeter enables or restricts connection to, and communication with, the internet. To control network traffic, the organization should use devices such as border routers and firewalls to restrict and filter traffic. These tools should be securely configured and maintained with current operating systems. Protection controls such as network segmentation, firewalls, and physical access controls to network equipment can be utilized to strengthen the integrity and resilience of an organization. Network architecture and network services design gives specific consideration to resilience, integrity, and security factors. Design principles such as zero trust architecture can be used as an alternative to enhance the control network services.

Describe controls established (e.g., denial of service protections, secure name/address resolution, and/or alternate communications paths) to enhance the organization’s communications and control network services.

Examples of Effective Evidence:

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-087: Security Control and Process Improvement Documents

- Continuous improvement plans for security controls and processes, detailing objectives, actions, timelines, and responsible parties.
- Budget requests and justifications for improvement recommendations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of security control assessments, including findings and recommendations for enhancements.
- Change management records for updates to security processes and controls, including rationale and outcomes.
- Feedback collection mechanisms and reports from users and stakeholders on security controls, informing improvement plans.
- Performance metrics and monitoring reports that track the effectiveness of security controls and process improvements over time.

PR.IR-01.04: The organization controls access to its wireless networks and the information that these networks process by implementing appropriate mechanisms (e.g., strong authentication for authentication and transmission, preventing unauthorized devices from connecting to the internal networks, restricting unauthorized traffic, and segregating guest wireless networks).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #architecture | #authentication | #authorization | #boundary_protection | #infrastructure_protection | #network_diagrams | #network_segmentation

Response Guidance:

Wireless networks should include end-to-end encryption and strong authentication protocols (e.g., WPA2 + AES). Appropriate controls should exist on any wireless network to prevent unauthorized traffic from entering the network by appropriately segregating wireless and guest wireless networks.

Provide information as to how the organization controls access to its wireless networks and the information that these networks process. Describe the mechanisms and tools utilized (e.g., appropriate authentication protocols).

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PR.IR-01.05: Remote access is carefully controlled (e.g., restricted to defined systems, access is actively managed (e.g., session timeouts, logging, forced disconnect, etc.), and encrypted connections with multi-factor authentication are used).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authentication | #authorization | #encryption | #identity_and_access_management | #multi_factor_authentication | #remote_access | #session_management

Response Guidance:

Remote access enables network troubleshooting, updates, and maintenance. Security controls (e.g., encryption, access roles and privileges, strong authentication, patching, access logging, auditing) should be in place to effectively protect against the numerous risks that remote access poses to the organization. Controlled and restricted remote access should include network and system administrators. Remote access should have encrypted connections with multi-factor authentication. Describe how the organization implements multi-factor authentication or equally secure access controls for remote access.

Describe how remote access is carefully controlled and restricted to necessary systems. Necessary systems may include components, applications and/or devices. Describe how all types of external connections into the corporate network (e.g., employees, third-parties, virtual, desktops, etc.) are carefully controlled and restricted to necessary systems.

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

EEE-057: Remote Access Security and Management Documentation

- Policies governing remote access to the organization's network and systems, including user authentication and authorization procedures and end-user acceptable use policies.
- Records of remote access configurations and settings, ensuring secure connections (e.g., VPN configurations).
- Audit trails or logs of remote access sessions, including user activities and access times.
- Reviews or assessments of remote access security controls, identifying any gaps or improvements needed.
- Training records for employees and contractors on secure remote access practices.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PR.IR-01.06: The organization's production and non-production environments and data are segregated and managed to prevent unauthorized access or changes to the information assets.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #architecture | #data_protection | #encryption | #identity_and_access_management | #network_segmentation | #separation_of_duties

Response Guidance:

Separation of non-production (e.g., development) from the production environment is important to safeguarding the confidentiality and integrity of information. Production data must be maintained with the same level of control if used for acceptance testing. All environments must maintain strong security controls, and movement of code or data between environments should be protected.

Provide information on how the organization's production is separate from the non-production environment (logically/physically). Provide information on the network segmentation. Describe how data (both non-production and production) is protected, managed, and not used in inappropriate environments to prevent unauthorized access or changes to the information assets. Describe the access controls established to ensure that developers, administrators, and other privileged users reduce the exposure to production data. In particular, the organization's controls in place for backdoor production data changes and corrections that need to be made and documented.

Examples of Effective Evidence:

EEE-010: IT Asset Management and Business Function Mapping Documentation

- Inventory list of IT assets, including hardware, software, and data.
- Business function catalog that maps key assets to their corresponding business process.
- Asset ownership and stewardship records indicating who is responsible for specific assets.
- Lifecycle management records for assets, showing purchase dates, warranty periods, and disposal information.
- Integration diagrams showing how assets interact within the business's technology ecosystem.

PR.IR-01.07: The organization defines and implements controls for securely configuring and operating Operational Technologies, Industrial Control Systems, and Internet-of-Things (IoT) devices (e.g., segregated printer networks, resetting of default passwords, etc.)

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #emerging_technologies | #network_segmentation | #patch_management | #security_baselines | #system_hardening

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

The organization should define, implement, and actively manage controls for securely configuring and operating Operational Technologies, Industrial Control Systems, and Internet-of-Things (IoT) devices. Organizations should maintain an inventory of Operational Technologies, Industrial Control Systems, and Internet-of-Things (IoT) devices. In financial institution environments, operational technologies generally include services such as printers, faxes, ATM's, cash management devices, security systems, video surveillance systems, and audio/video conference systems. Baseline configuration should be defined and established for Industrial Control Systems and network of connected devices to maintain security principles throughout configuration. Organizations should use a segmented network for Operational Technologies, as appropriate. Effective policies, procedures, and security controls should be implemented to mitigate risk and potential vulnerabilities. Describe security standards in place for operating all types of assets including Operational Technologies, Industrial Control Systems, and Internet-of-Things (IoT) devices.

Describe how controls are defined and implemented for securely configuring and operating devices (e.g., physical access controls, least functionality). Describe standards, and controls in place for physical access security of operating Operational Technologies, Industrial Control Systems, and Internet-of-Things (IoT) devices.

Examples of Effective Evidence:

EEE-056: Operational Technology and IoT Security Documentation

- Security policies and procedures specific to operational technology (OT) and Internet of Things (IoT) devices.
- Inventory lists of OT and IoT devices, including security features and firmware versions.
- Risk assessments for OT and IoT devices, identifying potential vulnerabilities and mitigation strategies.
- Configuration standards for various types of OT and IoT devices (e.g., default password reset).
- Incident response plans that include protocols for addressing security incidents involving OT and IoT devices.
- Documentation of security patches and updates applied to OT and IoT devices, along with testing results.

EEE-087: Security Control and Process Improvement Documents

- Continuous improvement plans for security controls and processes, detailing objectives, actions, timelines, and responsible parties.
- Budget requests and justifications for improvement recommendations.
- Documentation of security control assessments, including findings and recommendations for enhancements.
- Change management records for updates to security processes and controls, including rationale and outcomes.
- Feedback collection mechanisms and reports from users and stakeholders on security controls, informing improvement plans.
- Performance metrics and monitoring reports that track the effectiveness of security controls and process improvements over time.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

PR.IR-01.08: The organization implements policies, procedures, end-user agreements, and technical controls to address the risks of end-user mobile or personal computing devices accessing the organization's network and resources.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #end_user_security | #endpoint_security | #infrastructure_protection | #mobile_device_management | #patch_management | #policy_management

Response Guidance:

Provide information on established policies, procedures, and end-user agreements for defining and permitting use of acceptable technology, social media, and personal devices for all personnel (employees and third party). Describe how the acceptable use policies, procedures, and agreements permit access to the organization's information systems and networks. Inappropriate use exposes the organization to potential risks (e.g., unauthorized access, compromise of network systems). Describe technical controls (e.g., VPN, antivirus software, password requirements) implemented to address the risks of end-user mobile and/or personal computing devices accessing the organization's network and resources.

Describe how the organization implements mechanisms to restrict access to websites or services that do not serve legitimate business needs or purposes. Provide information on approval and authorization processes for all personnel to access the organization's applications and network through personnel devices. Describe the process of all personnel reviewing and accepting acceptable use policies.

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

EEE-057: Remote Access Security and Management Documentation

- Policies governing remote access to the organization's network and systems, including user authentication and authorization procedures and end-user acceptable use policies.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of remote access configurations and settings, ensuring secure connections (e.g., VPN configurations).
- Audit trails or logs of remote access sessions, including user activities and access times.
- Reviews or assessments of remote access security controls, identifying any gaps or improvements needed.
- Training records for employees and contractors on secure remote access practices.

EEE-074: Data Protection and Encryption Documentation

- Consolidated data protection policies that mandate encryption for sensitive data, detailing standards and handling procedures.
- Certificates and reports demonstrating compliance with recognized encryption standards.
- Centralized records of encryption solutions implemented across the organization, including configuration details.
- Integrated data breach response and incident management plans that specify the use of encryption as a protective measure.
- Streamlined training documentation for all employees on data protection and encryption best practices.

PROTECT / Technology Infrastructure Resilience / Environmental Threat Protections

PR.IR-02.01: The organization designs, documents, implements, tests, and maintains environmental and physical controls to meet defined business resilience requirements (e.g., environmental monitoring, dual power and communication sources, regionally separated backup processing facilities, etc.)

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #critical_infrastructure | #data_backup | #facilities_management | #physical_security | #policy_management | #resilience | #risk_management | #technology_availability

Response Guidance:

Environmental and physical controls (e.g., temperature and humidity controls or water damage protection for data centers or server rooms) ensure the availability of the organization's systems. Physical access controls for data centers should have surveillance controls at entry points, exit points, and inside, as well as geographical location controls to ensure faster latency, and recovery. The organization's environmental and physical controls should be designed according to resilience strategies and framework, and technology architecture in place. Physical controls should control and restrict entry and exit to organization's areas including, entry points in barriers, keycard-controlled doors, screening measures at entry points, and training for personnel who work in sensitive areas, etc. Environment controls should help organization's operate at a reasonably well-controlled environment, including fire suppression and detection devices, automatic emergency lighting during power outages, etc.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Describe how environmental and physical controls are designed, documented, implemented, tested, and maintained to meet defined business resilience requirements. Provide testing performed on environmental and physical controls to ensure effectiveness.

Examples of Effective Evidence:

EEE-077: Physical and Environmental Security Documents

- Documentation of environmental controls (e.g., fire suppression, climate control) and physical security measures (e.g., access controls, surveillance systems).
- Maintenance and inspection records for environmental and physical security equipment.
- Incident logs related to environmental hazards or physical security breaches, including responses and outcomes.
- Security audit reports evaluating the adequacy of environmental and physical security controls.

PROTECT / Technology Infrastructure Resilience / Resilience Measures

PR.IR-03.01: The organization implements mechanisms (e.g., failsafe, load balancing, hot swaps, redundant equipment, alternate services, backup facilities, etc.) to achieve resilience requirements in normal and adverse situations.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #architecture | #critical_infrastructure | #data_backup | #disaster_recovery | #hotswap | #incident_management | #resilience | #technology_availability

Response Guidance:

Describe how the organization implements mechanisms (e.g., failsafe, load balancing, hot swap, redundant equipment, alternate sites, backup facilities, etc.) to achieve resilience requirements in normal and adverse situations. Mechanisms should be established to ensure the organization can resume critical business services after disruption. For example, backup facilities can be used for resumption of services when critical services are disrupted, or data is rendered corrupted, or inaccessible. The organization's mechanisms should be designed according to resilience strategies, and technology architecture in place. Provide information on risk assessment and tier strategy where applicable. Provide implementation strategy information related to normal vs. adverse situations.

Examples of Effective Evidence:

EEE-013: Operational Resilience and Continuity Procedures Documentation

- Standard operating procedures (SOPs) for responding to incidents that threaten resilience and continuity.
- Business continuity plan outlining procedures for maintaining service delivery during disruptions.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Recovery time objectives (RTOs), recovery point objectives (RPOs), maximum tolerable downtime (MTO), impact tolerance, and/or other recovery objective metrics are established for key services.
- Communication plans for stakeholders during a service disruption, to include alternative communication mechanisms.
- Contingency plans detailing alternative service delivery methods.
- Training records for staff on resilience and continuity procedures and their roles during incidents.

EEE-014: Resilience and Continuity Design and Assessment Documents

- A documented methodology for evaluating the resilience and continuity of business operations and IT systems.
- Workbooks or diagrams that visually depict the dependencies of critical business processes.
- Risk impact studies with mitigation strategies for critical functions.
- Meeting minutes from design reviews focused on enhancing system resilience and continuity.
- Industry benchmarking reports comparing the organization's resilience and continuity capabilities.
- Checklists used for auditing the content and coverage of resilience and continuity plans.

EEE-029: Critical Function Resilience Documentation

- Plans that specifically address the continuity and resilience of critical business functions.
- Dashboards or reports that monitor the health and resilience of critical functions.
- Definitions of measures used to manage and assess resilience (RPO, RTO, MTO, Impact Tolerance, etc.)
- Documentation of resilience requirements integrated into the design of new services or processes.
- Evaluations or audits of the resilience program, highlighting strengths and areas for improvement.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-059: Enterprise and Cyber Resilience Policy Documentation

- Official enterprise resilience strategy documents that outline the organization's approach to achieving and maintaining resilience.
- Cyber resilience policy documents that specify the measures and controls in place to protect against cyber threats.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Board presentations and approvals related to the resilience strategy and cyber resilience policies.
- Reports from resilience assessments, including gap analyses and recommendations for improvement.

EEE-090: Security and Resilience Design Standards Documents

- Official documents outlining security and resilience architectural and design standards that all technology projects and initiatives must adhere to.
- Checklists and templates used during the design phase of projects to ensure compliance with security and resilience standards.
- Records of design review sessions where security and resilience considerations were evaluated and enforced.
- Case studies or examples of projects that successfully implemented these design standards.
- Audit or review reports assessing adherence to security and resilience design standards across projects.

EEE-100: Resilience Testing and Business Impact Documentation

- Resilience testing plans and procedures, including objectives and expected outcomes.
- Business Impact Assessment (BIA) reports that evaluate the potential effects of disruptions on business operations.
- Records of resilience testing exercises, including scenarios, execution, and lessons learned.
- Documentation of updates to resilience plans based on testing outcomes and BIA findings.
- Stakeholder feedback on the organization's resilience and the impact of potential business disruptions.

PROTECT / Technology Infrastructure Resilience / Capacity Management

PR.IR-04.01: Baseline measures of network and system utilization and transaction activity are captured to support capacity planning and anomalous activity detection.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #architecture | #security_logging_monitoring_and_alerting

Response Guidance:

Organizations should maintain baseline measures of network, system utilization and transaction activity that are captured to support capacity planning and anomalous activity detection. The organization should identify hardware, software, and network components, internal and external connections, and types of information passed between systems to facilitate the development of a defense-in-depth security architecture and ensure appropriate network security. Network diagrams should be comprehensive, up-to-date and include inventoried assets.

Processes and procedures should describe how the organization identifies, establishes, documents, and manages a baseline measure of network, system utilization, and transaction activity. Provide information supporting mapping of resources, connections, and data flows. Describe the organization’s use of operational and network monitoring tools in the environment. Describe how

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

operational and network monitoring intersect with event detection, incident identification, and incident management processes.

Examples of Effective Evidence:

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-079: Capacity Planning and Resource Utilization Documentation

- Capacity planning strategies and models that forecast infrastructure and resource needs based on business growth and demand.
- Utilization monitoring reports and dashboards that track the usage of IT resources and infrastructure.
- Documentation of actions taken to address capacity constraints or optimize resource utilization.
- Reviews or assessments of capacity planning and utilization monitoring practices, identifying opportunities for optimization.

EEE-080: Intrusion Detection and Prevention Systems (IDPS) Documentation

- Policies and procedures governing the operation of intrusion detection and prevention systems (IDPS).
- Configuration and management records for IDPS, detailing rule sets, detection mechanisms, and response actions.
- Logs and alerts generated by IDPS, including analysis of detected intrusions and the effectiveness of prevention measures.
- Audit or review reports assessing the coverage, configuration, and effectiveness of intrusion detection and prevention measures.

PR.IR-04.02: Technology availability and capacity is planned, monitored, managed, and optimized to meet business resilience objectives and reasonably anticipated infrastructure demands.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #critical_infrastructure | #resilience | #security_logging_monitoring_and_alerting | #technology_availability

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Provide information on how the organization maintains appropriate technology availability and capacity. Describe how the organization plans, monitors, manages, and optimizes technology availability and capacity to meet resilience objectives and reasonably anticipated infrastructure demands. Describe the linkage to availability requirements and risk assessment. Describe service level management and baselines including any scheduled downtime.

Examples of Effective Evidence:

EEE-054: Technology Service Performance and Support Monitoring Documentation

- Service level agreements (SLAs) and key performance indicators (KPIs) for technology services and support functions.
- Documentation for service catalogs, service support systems, or other mechanisms for end-users to request services.
- Monitoring dashboards or reports that track service performance against SLAs and KPIs.
- Records of service incidents, including response times, resolution details, and customer feedback.
- Procedures for managing and improving technology service performance.

EEE-079: Capacity Planning and Resource Utilization Documentation

- Capacity planning strategies and models that forecast infrastructure and resource needs based on business growth and demand.
- Utilization monitoring reports and dashboards that track the usage of IT resources and infrastructure.
- Documentation of actions taken to address capacity constraints or optimize resource utilization.
- Reviews or assessments of capacity planning and utilization monitoring practices, identifying opportunities for optimization.

EEE-080: Intrusion Detection and Prevention Systems (IDPS) Documentation

- Policies and procedures governing the operation of intrusion detection and prevention systems (IDPS).
- Configuration and management records for IDPS, detailing rule sets, detection mechanisms, and response actions.
- Logs and alerts generated by IDPS, including analysis of detected intrusions and the effectiveness of prevention measures.
- Audit or review reports assessing the coverage, configuration, and effectiveness of intrusion detection and prevention measures.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

DETECT / Continuous Monitoring / Network Monitoring

DE.CM-01.01: The organization deploys intrusion detection and intrusion prevention capabilities to detect and prevent a potential network intrusion in its early stages for timely containment and recovery.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #boundary_protection | #infrastructure_security | #security_logging_monitoring_and_alerting

Response Guidance:

Intrusion detection or prevention systems, anti-virus software, and endpoint detection can be used to help identify unusual activity by analyzing network traffic or code and alerting or taking action (e.g., blocking traffic that enters the network). Intrusion detection or prevention systems may include detecting potential insider threat activity. For example, incidents that may relate to insider threat may include failed log-in attempts, transfers of large amounts of data, altered coding on sensitive files, or personnel issues.

Describe both host and network-based intrusion detection and prevention capabilities deployed to detect and prevent a potential network intrusion in its early stages for timely response, containment, and recovery. Provide information regarding the layers of protection.

Examples of Effective Evidence:

EEE-027: Security Event Detection and Categorization Guidelines

- Documentation of the security information and event management (SIEM) system configuration and operational procedures.
- Incident categorization guidelines that define types of incidents and their corresponding response protocols.
- Logs and reports from the SIEM system demonstrating the detection of security events.
- Training materials for security analysts on event detection and incident categorization.
- Audit trails showing the escalation process from event detection to incident declaration.

EEE-080: Intrusion Detection and Prevention Systems (IDPS) Documentation

- Policies and procedures governing the operation of intrusion detection and prevention systems (IDPS).
- Configuration and management records for IDPS, detailing rule sets, detection mechanisms, and response actions.
- Logs and alerts generated by IDPS, including analysis of detected intrusions and the effectiveness of prevention measures.
- Audit or review reports assessing the coverage, configuration, and effectiveness of intrusion detection and prevention measures.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

DE.CM-01.02: The organization implements mechanisms, such as alerting and filtering of sudden high volumes and suspicious incoming traffic, to detect and mitigate Denial of Service, "bot", and credential stuffing attacks.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #boundary_protection | #infrastructure_security | #security_logging_monitoring_and_alerting

Response Guidance:

Identification of disruptive cyber-attacks such as Denial of Service (DoS)/Distributed Denial of Service (DDoS) attacks relies on a coordinated collection and analysis of performance data and alerts, often including third-party providers such as upstream internet service providers (ISPs). Many risk-based tools are available to monitor uptime and system responsiveness. The organization should devise and implement mitigation approaches according to the organization's risk exposure.

Describe the mechanisms implemented to detect and mitigate Denial of Service, "bot", and credential stuffing attacks. Provide information on alerting and filtering procedures when experiencing a sudden high volume of suspicious incoming traffic.

Examples of Effective Evidence:

EEE-080: Intrusion Detection and Prevention Systems (IDPS) Documentation

- Policies and procedures governing the operation of intrusion detection and prevention systems (IDPS).
- Configuration and management records for IDPS, detailing rule sets, detection mechanisms, and response actions.
- Logs and alerts generated by IDPS, including analysis of detected intrusions and the effectiveness of prevention measures.
- Audit or review reports assessing the coverage, configuration, and effectiveness of intrusion detection and prevention measures.

DE.CM-01.03: The organization has policies, procedures, and tools in place to monitor for, detect, and block unauthorized network connections and data transfers.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #data_protection | #infrastructure_protection | #infrastructure_security | #policy_management | #security_logging_monitoring_and_alerting

Response Guidance:

The organization should have a comprehensive system for monitoring unauthorized access to systems, devices, components, and software. For example, automated processes or tools can detect and prevent changes to hardware or software and can alert management when certain attempted changes are executed.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Describe the tools used to monitor, detect, and block access from/to devices, network connections, data transfers and API activity. Provide information on the approved policies and procedures. Provide information on how the various tools achieve the security objectives.

Examples of Effective Evidence:

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-076: Network Infrastructure and Access Control Documentation

- Network architecture diagrams that detail the infrastructure layout and access control points.
- Configuration management records for network devices, demonstrating the implementation of access controls.
- Audit logs and reports verifying compliance with network access policies and procedures.
- Incident response records showing the effectiveness of network access controls in mitigating unauthorized access.

DE.CM-01.04: The organization has policies, procedures, and tools in place to monitor for, detect, and block access from/to devices that are not authorized or do not conform to security policy (e.g., unpatched systems).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #infrastructure_protection | #infrastructure_security | #patch_management | #policy_management | #security_logging_monitoring_and_alerting | #vulnerability_management

Response Guidance:

The organization should have a system for monitoring devices and connections that are not authorized or do not conform to security policy. For example, vulnerability scanning tools can monitor and detect unpatched systems, deny connection, and alert management. Organizations may employ device fingerprinting, certificates, or other methods to identify authorized devices.

Describe the tools used to monitor, detect, and block access from/to devices and connections. Provide information on the approved policies and procedures. Provide information on how the various tools achieve the requirement.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-036: Vulnerability Scanning and Patch Management Documentation

- Policy, standard, and/or procedure documents covering the identification, assessment, reporting, and remediation of software and device vulnerabilities, including regular patching protocols.
- Schedules and records of patch deployment activities, including system reboots, post-patch testing, dates, systems affected, and patching outcomes.
- Documentation of patching or upgrades to standard system configuration baselines.
- Reports from vulnerability scans or assessments that inform the patch management process.
- Incident reports related to vulnerabilities that were mitigated through patch management.
- Documentation and reporting of vulnerability mitigation targets.
- Records of exceptions to, assessments of, and approvals for cases where vulnerability mitigation targets or standards are not met.
- Records demonstrating the integration of patch management and change management practices.
- Approval and review documentation for patching protocols, including impact assessments and authorization records.
- Dashboards or tools used to monitor patch levels and patch application across the target environment.
- Post-implementation reviews and post-change evaluation reports assessing the impact and success of patches and any unintended consequences.
- Audit or review findings related to vulnerability management and patching practices with actions taken in response to findings.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-103: Security Policy Review and Update Documents

- Security policy review schedules and procedures, including criteria for making updates.
- Change logs or records documenting updates to security policies, including reasons for changes.
- Meeting minutes from stakeholder meetings, capturing input on proposed policy updates.
- Training records for staff on updated security policies and new security requirements.
- Audit or assessment reports that have led to revisions of security policies.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

DE.CM-01.05: The organization implements measures to detect and block access to unauthorized, inappropriate, or malicious websites and services (e.g. social media, messaging, file sharing).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #data_protection | #infrastructure_protection | #infrastructure_security | #social_media

Response Guidance:

Describe the measures (e.g., web-filtering tools) implemented to detect and block access to unauthorized, inappropriate, or malicious websites and services. Provide information on tools used. Describe the organization's policy for connections to file sharing sites (e.g., DropBox, Box, etc.), and any procedures allowed to request exceptions. Describe how users can request exceptions to site blocking when required for business purposes.

Examples of Effective Evidence:

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

DE.CM-01.06: The organization employs deception techniques and technologies (e.g., honeypots) to detect and prevent a potential intrusion in its early stages to support timely containment and recovery.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Subject Tags: #data_protection | #infrastructure_security | #security_logging_monitoring_and_alerting

Response Guidance:

As a component of its threat intelligence and analysis capabilities, organizations should employ deception techniques and technologies that can identify and report possible incidents to

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

management. Management should quickly involve appropriate personnel outlined in incident response plan to support timely containment and recovery. Authorized threat identification and analyses collected by such methods should be shared with the broader financial services and intelligence communities through approved information sharing forums.

Provide information on how the organization utilizes deception techniques and technologies to detect and prevent a potential intrusion. Describe the intrusion detection and prevention capabilities deployed to detect and prevent a potential network intrusion in its early stages for timely response, containment, and recovery. Provide information regarding the layers of protection.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-085: Vulnerability Mitigation and Incident Containment Documentation

- Procedures for mitigating vulnerabilities and containing incidents to prevent further damage or data loss.
- Documentation of vulnerability scans and assessments, including identified vulnerabilities and mitigation actions taken.
- Incident containment plans, detailing specific containment strategies for different types of security incidents.
- Records of incident response drills or exercises focusing on containment and mitigation strategies.
- Post-incident reports analyzing the effectiveness of containment and mitigation efforts, with recommendations for improvement.

EEE-096: Incident Detection and Response Coordination Documentation

- Incident detection policies and procedures that define how potential security events are identified and analyzed.
- Coordination plans that outline roles and communication protocols for responding to incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Logs and reports from detection tools and systems, including details of incident analysis and response actions.
- Training and exercise records for response teams, demonstrating preparedness and coordination effectiveness.
- After-action reports and lessons learned from incident responses, used to improve future coordination.

DETECT / Continuous Monitoring / Physical Environment Monitoring

DE.CM-02.01: The organization's controls include monitoring and detection of anomalous activities and potential intrusion events across the organization's physical environment and infrastructure, including the detection of environmental threats (fire, water, service outages, etc.) and unauthorized physical access to high-risk system components and locations.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #boundary_protection | #critical_infrastructure | #physical_security | #security_logging_monitoring_and_alerting

Response Guidance:

Organizations should utilize monitoring and detection mechanisms and tools for the physical environment (e.g., entrances, restricted areas, confidential data repositories, vault areas, ATMs, etc.) and infrastructure, including any cloud infrastructure, if applicable.

Describe how the organization’s controls include monitoring and detection of anomalous activities and potential intrusion events across the organization's physical environment and infrastructure. Provide information on controls that detect environmental threats. Provide information on controls that detect unauthorized physical access to high-risk system components and locations (e.g., data centers, LAN closets, network cabling, etc.).

Examples of Effective Evidence:

EEE-077: Physical and Environmental Security Documents

- Documentation of environmental controls (e.g., fire suppression, climate control) and physical security measures (e.g., access controls, surveillance systems).
- Maintenance and inspection records for environmental and physical security equipment.
- Incident logs related to environmental hazards or physical security breaches, including responses and outcomes.
- Security audit reports evaluating the adequacy of environmental and physical security controls.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

DETECT / Continuous Monitoring / Personnel Activity Monitoring

DE.CM-03.01: Account access, authentication, and authorization activities are logged and monitored, for both users and devices, to enforce authorized access.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authentication | #authorization | #identity_and_access_management | #security_logging_monitoring_and_alerting

Response Guidance:

The organization should identify and perform logging of account access, authentication, and authorization activities. Appropriate access controls and monitoring procedures should be in place to alert of unauthorized access.

Describe how the organization performs logging to access control activities. Provide information of established logging and monitoring policies, standards, and procedures. Provide information regarding explicit approval and logging processes and alerts in place to enforce authorized access. Describe how system-to-system access activities are logged and monitored.

Examples of Effective Evidence:

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-076: Network Infrastructure and Access Control Documentation

- Network architecture diagrams that detail the infrastructure layout and access control points.
- Configuration management records for network devices, demonstrating the implementation of access controls.
- Audit logs and reports verifying compliance with network access policies and procedures.
- Incident response records showing the effectiveness of network access controls in mitigating unauthorized access.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

DE.CM-03.02: The organization's controls actively monitor personnel (both authorized and unauthorized) for access, authentication, usage, connections, devices, and anomalous behavior to rapidly detect potential cybersecurity events.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #authentication | #authorization | #identity_and_access_management | #infrastructure_protection | #security_logging_monitoring_and_alerting

Response Guidance:

The organization should have a comprehensive system for monitoring access to critical and mission critical systems, devices, components, software, and data for unauthorized access.

Describe what controls are in place to actively monitor users (both authorized and unauthorized) for access, authentication, usage, connections, devices, and anomalous behavior to rapidly detect potential cybersecurity events. Describe any tools employed to monitor user activity within the environment. Describe the organization's monitoring controls interaction with the insider threat program.

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

DE.CM-03.03: The organization logs and reviews the activities of privileged users and accounts, and monitoring for anomalous behaviors is implemented.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #identity_and_access_management | #privileged_access | #security_logging_monitoring_and_alerting

Response Guidance:

The organization should identify and perform logging of key systems, applications and devices and review logs on a regular basis, based on the risk profile of the organization. The organization should maintain a list of privileged users, and review and update the list of privileged users on a regular basis in accordance with the organization's policies and procedures.

Describe how the organization performs logging and monitoring. Provide information regarding the review of system activities of privileged users and accounts, and how monitoring for anomalous behavior is implemented. Describe any tools used specifically to manage privileged accounts (e.g., firecall access controls).

Examples of Effective Evidence:

EEE-035: Access Control and Identity Management Documentation

- Written policies and procedures detailing access control measures and identity management protocols.
- System configuration snapshots or reports demonstrating the implementation of access controls.
- Descriptions of role-based groups or other practices used to differentiate access rights.
- Records demonstrating regular review of access controls, authorized users, and least privilege principle application by system owners.
- Audit logs showing user access activities and adherence to access policies.
- Records of user account creation, modification, and termination processes.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

DETECT / Continuous Monitoring / Service Provider Monitoring

DE.CM-06.01: The organization reviews, documents, authorizes, and monitors all third-party connections, data transfer mechanisms, and Application Programming Interfaces (APIs).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #application_security | #architecture | #data_protection | #infrastructure_protection | #security_logging_monitoring_and_alerting | #third_party_risk_management | #supply_chain_management

Response Guidance:

The organization should have a process for documenting, reviewing, and approving external connections, reviewing, and approving external connections, data transfer, and APIs to ensure that appropriate security and resilience design is in place. Organizations should establish ongoing monitoring requirements to control and monitor all third-party connections, data transfer mechanisms, and application programming interfaces (APIs). Controls may include network segmentation, in-line intrusion detection systems/intrusion prevention systems, security information and event management (SIEM), or log aggregation tools, among others. There should be evidence that each third-party service has been formally approved (e.g., through signed contracts and Board meeting minutes). Further, back up connections should be tested to ensure resiliency and limit outage risk.

Describe how the organization reviews, documents, authorizes, and monitors all third-party connections, data transfer mechanisms, and APIs. Provide information regarding the process. Provide information of related policies, standards, and processes.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

DE.CM-06.02: The organization implements an explicit approval and logging process and sets up automated alerts to monitor and prevent any unauthorized access to a critical system by a third-party service provider.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #critical_infrastructure | #security_logging_monitoring_and_alerting | #third_party_risk_management | #supply_chain_management

Response Guidance:

Appropriate access controls and monitoring should be in place between the organization and service provider systems and employees. The organization should have procedures in place detailing specific activities that are authorized by third-party service providers and systems which monitor and alert on unauthorized activity.

Describe what the organization has implemented with regards to explicit approval and logging processes and alerts to monitor and prevent any unauthorized access to a critical system by a third-party service provider.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

DETECT / Continuous Monitoring / Hardware, Software, & Data Monitoring

DE.CM-09.01: The organization uses integrity checking mechanisms to verify software, firmware and information integrity and provenance (e.g., checksums, Software Bill of Materials, etc.)

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #application_security | #data_protection | #security_logging_monitoring_and_alerting | #system_integrity | #vulnerability_management

Response Guidance:

Describe how the organization uses information security integrity checking mechanisms to verify the integrity and provenance of software, and firmware. Provide information on the various mechanisms in place and how they are used for software, firmware, and information integrity and provenance. For example, information security integrity checking mechanisms may include file integrity monitoring, checksums, credential changes, hash value changes, etc.

Examples of Effective Evidence:

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

DE.CM-09.02: The organization uses integrity checking mechanisms to verify hardware integrity.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #application_security | #data_protection | #security_logging_monitoring_and_alerting | #system_integrity | #vulnerability_management

Response Guidance:

Describe how the organization uses integrity checking mechanisms to verify hardware integrity. Provide information on the types of mechanisms used.

Refer to PR.DS-6.1 for more information on using integrity checking mechanisms to verify software, firmware, and information integrity.

Examples of Effective Evidence:

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

DE.CM-09.03: The organization has policies, procedures, and tools in place to monitor for, detect, and block the use of unsupported or unauthorized software, hardware, or configuration changes.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #endpoint_security | #infrastructure_protection | #policy_management | #security_baselines | #security_logging_monitoring_and_alerting | #vulnerability_management

Response Guidance:

Unauthorized software, hardware, or configuration changes introduces significant risk to the organization, as actors can gain access to sensitive data. The organization should implement controls to monitor, scan, detect, and block unauthorized changes to protect integrity of software, hardware, and firmware.

Unsupported operating systems and components also may introduce significant risk to the organization, as updates, patches and fixes are no longer available. The organization should implement compensating controls to protect against the threats of unsupported systems.

Describe what policies, procedures, and tools have been implemented to monitor, detect, and/or block the use of unsupported and unauthorized software, hardware, or configuration changes. Provide information on the configuration, software, and hardware management processes.

Examples of Effective Evidence:

EEE-036: Vulnerability Scanning and Patch Management Documentation

- Policy, standard, and/or procedure documents covering the identification, assessment, reporting, and remediation of software and device vulnerabilities, including regular patching protocols.
- Schedules and records of patch deployment activities, including system reboots, post-patch testing, dates, systems affected, and patching outcomes.
- Documentation of patching or upgrades to standard system configuration baselines.
- Reports from vulnerability scans or assessments that inform the patch management process.
- Incident reports related to vulnerabilities that were mitigated through patch management.
- Documentation and reporting of vulnerability mitigation targets.
- Records of exceptions to, assessments of, and approvals for cases where vulnerability mitigation targets or standards are not met.
- Records demonstrating the integration of patch management and change management practices.
- Approval and review documentation for patching protocols, including impact assessments and authorization records.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Dashboards or tools used to monitor patch levels and patch application across the target environment.
- Post-implementation reviews and post-change evaluation reports assessing the impact and success of patches and any unintended consequences.
- Audit or review findings related to vulnerability management and patching practices with actions taken in response to findings.

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.
- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.
- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

DETECT / Adverse Event Analysis / Potentially Adverse Event Analysis

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

DE.AE-02.01: The organization performs timely collection of event data, as well as advanced and automated analysis (including the use of security tools such as antivirus and IDS/IPS) on the detected events to:

(1) Assess and understand the nature, scope and method of the attack;

(2) Predict and block a similar future attack; and

(3) Report timely risk metrics.

Subject Tags: #boundary_protection | #endpoint_security | #malware_protection | #security_logging_monitoring_and_alerting | #siem

Response Guidance:

Proactive cyber risk management involves developing threat intelligence capabilities based upon data collection and metrics. Organizations should use network-monitoring software to detect internal and external cyber threats and have system event and antivirus systems configured to alert management and/or appropriate security personnel when an event is detected. For example, a security information and event management (SIEM) tool may be used to correlate data and manage events.

Describe how the organization performs timely collection of event data, as well as advanced and automated analysis (including use of security tools such as antivirus and intrusion detection systems (IDS) / intrusion prevention systems (IPS)) on the detected events. Describe the tools used and how the data collection and analysis is utilized to: (1) assess and understand the nature, scope, and method of the attack; (2) predict and block a similar future attack; and (3) report timely risk metrics.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-027: Security Event Detection and Categorization Guidelines

- Documentation of the security information and event management (SIEM) system configuration and operational procedures.
- Incident categorization guidelines that define types of incidents and their corresponding response protocols.
- Logs and reports from the SIEM system demonstrating the detection of security events.
- Training materials for security analysts on event detection and incident categorization.
- Audit trails showing the escalation process from event detection to incident declaration.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-080: Intrusion Detection and Prevention Systems (IDPS) Documentation

- Policies and procedures governing the operation of intrusion detection and prevention systems (IDPS).
- Configuration and management records for IDPS, detailing rule sets, detection mechanisms, and response actions.
- Logs and alerts generated by IDPS, including analysis of detected intrusions and the effectiveness of prevention measures.
- Audit or review reports assessing the coverage, configuration, and effectiveness of intrusion detection and prevention measures.

DE.AE-02.02: The organization establishes, documents, and regularly reviews event alert parameters and thresholds, as well as rule-based triggers to support automated responses, when known attack patterns, signatures or behaviors are detected.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #incident_management | #security_logging_monitoring_and_alerting

Response Guidance:

Conditions to scan for in log data should be defined to alert on potentially adverse events. Parameters or thresholds should be established to provide alerts and notifications to the proper

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

personnel when those thresholds are exceeded. For example, an exception report can be used to document when a threshold has been exceeded.

Describe how the organization establishes, documents, and regularly reviews event alert parameters and thresholds, as well as rule-based triggers to support automated responses, when known attack patterns, signatures or behaviors are detected.

Examples of Effective Evidence:

EEE-027: Security Event Detection and Categorization Guidelines

- Documentation of the security information and event management (SIEM) system configuration and operational procedures.
- Incident categorization guidelines that define types of incidents and their corresponding response protocols.
- Logs and reports from the SIEM system demonstrating the detection of security events.
- Training materials for security analysts on event detection and incident categorization.
- Audit trails showing the escalation process from event detection to incident declaration.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

DETECT / Adverse Event Analysis / Event Information Correlation

DE.AE-03.01: The organization implements systematic and real-time logging, collection, monitoring, detection, and alerting measures across multiple layers of the organization's infrastructure, including physical perimeters, network, operating systems, applications, data, and external (cloud and outsourced) environments, sufficient to protect the organization's information assets.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #application_security | #boundary_protection | #data_protection | #endpoint_security | #incident_management | #infrastructure_protection | #security_logging_monitoring_and_alerting | #siem

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Protecting organizations from cyber threats requires constant vigilance over security infrastructure and critical information assets. Real time or near real-time security logs and alerts help identify and thwart malicious activity. Systems must balance numerous ongoing operational and strategic security tasks. The organization should implement device and network monitoring technologies that provide actionable information to inform and support incident response. Organizations should also monitor the physical environment (e.g., entrances, restricted areas, confidential data repositories, vault areas, ATMs, etc.).

Describe how the organization has implemented systematic and real-time/near real-time logging, collection monitoring, detection, and alerting measures across multiple layers of the organization's infrastructure and external environments, that produce actionable information sufficient to protect the organization's information assets. Describe the methodology and tools utilized to cover physical perimeters, network, operating systems, applications, and data.

Examples of Effective Evidence:

EEE-027: Security Event Detection and Categorization Guidelines

- Documentation of the security information and event management (SIEM) system configuration and operational procedures.
- Incident categorization guidelines that define types of incidents and their corresponding response protocols.
- Logs and reports from the SIEM system demonstrating the detection of security events.
- Training materials for security analysts on event detection and incident categorization.
- Audit trails showing the escalation process from event detection to incident declaration.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-049: Vulnerability Disclosure and Response Protocol Documentation

- Procedures for receiving, assessing, and responding to vulnerability disclosures from external researchers, customers, or other entities.
- Communication templates and protocols for interacting with individuals or organizations reporting vulnerabilities.
- Records of disclosed vulnerabilities, including the organization's response and remediation actions.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Agreements or MOUs with bug bounty platforms or security researchers regarding vulnerability disclosure.
- Reports summarizing the outcomes of vulnerability disclosures and the effectiveness of the response process.

EEE-102: Vulnerability Disclosure Management Documentation

- Vulnerability disclosure policies that define how external reports of potential vulnerabilities are managed and addressed.
- Documentation of vulnerability disclosures received, including the organization's response and remediation efforts.
- Communication records with security researchers or reporting parties regarding vulnerability disclosures.
- Reports summarizing the outcomes of vulnerability disclosures and the effectiveness of the response process.

DE.AE-03.02: The organization performs real-time central analysis, aggregation, and correlation of anomalous activities, network and system alerts, and relevant event and cyber threat intelligence, including both internal and external (cloud and outsourced) environments, to better detect and prevent multifaceted cyber attacks.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #security_logging_monitoring_and_alerting | #siem | #threat_management

Response Guidance:

The organization should deploy tools, as appropriate, to collect and aggregate information, including threat intelligence, to provide a holistic view of the organization's security posture. The organization should monitor network traffic in real-time with automated tools in order to detect internal and external cyber threats. For example, a security information and event management (SIEM) tool can be used to collect and log security-related documentation for analysis and correlation.

Describe the tools utilized to perform real-time central analysis, aggregation, and correlation of anomalous activities, network and system alerts, and relevant event and cyber threat intelligence from multiple sources, including both internal and external sources, to better detect and prevent multifaceted cyber-attacks.

Examples of Effective Evidence:

EEE-027: Security Event Detection and Categorization Guidelines

- Documentation of the security information and event management (SIEM) system configuration and operational procedures.
- Incident categorization guidelines that define types of incidents and their corresponding response protocols.
- Logs and reports from the SIEM system demonstrating the detection of security events.
- Training materials for security analysts on event detection and incident categorization.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Audit trails showing the escalation process from event detection to incident declaration.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-049: Vulnerability Disclosure and Response Protocol Documentation

- Procedures for receiving, assessing, and responding to vulnerability disclosures from external researchers, customers, or other entities.
- Communication templates and protocols for interacting with individuals or organizations reporting vulnerabilities.
- Records of disclosed vulnerabilities, including the organization's response and remediation actions.
- Agreements or MOUs with bug bounty platforms or security researchers regarding vulnerability disclosure.
- Reports summarizing the outcomes of vulnerability disclosures and the effectiveness of the response process.

EEE-102: Vulnerability Disclosure Management Documentation

- Vulnerability disclosure policies that define how external reports of potential vulnerabilities are managed and addressed.
- Documentation of vulnerability disclosures received, including the organization's response and remediation efforts.
- Communication records with security researchers or reporting parties regarding vulnerability disclosures.
- Reports summarizing the outcomes of vulnerability disclosures and the effectiveness of the response process.

DETECT / Adverse Event Analysis / Impact & Scope Determination

DE.AE-04.01: The organization has a documented process to analyze and triage incidents to assess root cause, technical impact, mitigation priority, and business impact on the organization, as well as across the financial sector and other third party stakeholders.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #forensics | #incident_management | #information_sharing | #lessons_learned | #root_cause_analysis

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

The organization should have processes in place for analyzing the impact associated with cybersecurity incidents. The significance of cybersecurity risks depends upon their nature, extent, potential magnitude, and the range of harm such incidents could cause to the organization's reputation, financial performance, customer relations, and impact across the financial sector.

Describe the documented process to analyze and triage incidents to assess root cause, technical impact, mitigation priority, the impact of a significant cybersecurity incident, as defined by the organization's risk appetite. Describe how the process for the organization to analyze and triage considering the financial impact across the financial sector, as appropriate, per the organization's size, scope, complexity, and role in the financial sector. Provide information on the organization's defined and established incident thresholds. Describe the documented process in place to analyze and triage incidents based on the potential business impact on other third party stakeholders.

Examples of Effective Evidence:

EEE-028: Investigation and Forensic Documentation

- Standard operating procedures (SOPs) for conducting security investigations and handling forensic data.
- Chain of custody forms and logs that track the handling and analysis of forensic evidence.
- Forensic toolkits and software licenses used for data analysis during investigations.
- Forensic investigation reports detailing the rigor of methods applied.
- Training certifications and other qualifications for personnel or third parties involved in forensic investigations.
- Reports from completed investigations, including methodologies, findings, and recommendations.

EEE-081: Incident Analysis and Triage Process Documentation

- Documentation of standardized processes for analyzing and triaging security incidents, including criteria for categprization and prioritization.
- Logs and reports from incident management systems showing the application of triage processes in real incidents.
- After-action reviews or lessons learned documents from incidents, highlighting the effectiveness of analysis and triage procedures.
- Continuous improvement plans based on feedback and performance metrics from incident analysis activities.

EEE-100: Resilience Testing and Business Impact Documentation

- Resilience testing plans and procedures, including objectives and expected outcomes.
- Business Impact Assessment (BIA) reports that evaluate the potential effects of disruptions on business operations.
- Records of resilience testing exercises, including scenarios, execution, and lessons learned.
- Documentation of updates to resilience plans based on testing outcomes and BIA findings.
- Stakeholder feedback on the organization's resilience and the impact of potential business disruptions.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

DETECT / Adverse Event Analysis / Event Information Sharing

DE.AE-06.01: The organization has established processes and protocols to communicate, alert, and regularly report potential cyber attacks and incident information, including its corresponding analysis and cyber threat intelligence, to authorized internal and external stakeholders.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #incident_management | #information_sharing | #security_logging_monitoring_and_alerting | #threat_management

Response Guidance:

Organizations should stay aware of highly visible cyber events through open-source reporting, industry alerts, law enforcement alerts, or regulatory alerts. The organization's management should have processes in place for periodically reporting incident information within the organization, to staff, management, and the Board. The organization should also have processes in place for sharing threat and incident data with external stakeholders (e.g., clients, regulators, law enforcement, etc.) to benefit the financial sector by enabling other organizations to assess and respond to current attacks.

Describe the established processes and escalation protocols to communicate, alert and regularly report potential cyber attacks and incident information, including the corresponding analysis and cyber threat intelligence, to authorized internal and external stakeholders.

Examples of Effective Evidence:

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

DETECT / Adverse Event Analysis / Contextual Analysis

DE.AE-07.01: The organization implements measures for monitoring external sources (e.g., social media, the dark web, etc.) to integrate with other intelligence information to better detect and evaluate potential threats and compromises.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #threat_management | #social_media

Response Guidance:

Organizations should stay current on cyber threat intelligence from both internal and external sources to achieve broader cybersecurity situational awareness and collect information about potential threats. Provide information about external sources monitored and ingested by the organization. Describe how external threat intelligence sources are integrated with other intelligence information. Provide information on established processes to gather and analyze relevant external cyber threat information.

Examples of Effective Evidence:

EEE-084: Cyber Threat Intelligence Sharing and Distribution Documents

- Policies and procedures for collecting, analyzing, and distributing cyber threat intelligence within the organization and with external partners.
- Agreements or memberships with threat intelligence sharing platforms or industry groups.
- Records of threat intelligence briefings or alerts issued to relevant stakeholders.
- Evaluations of the threat intelligence program, assessing its contribution to the organization's security posture.

EEE-101: Cyber Threat Intelligence Sharing Documentation

- Cyber threat intelligence policies that outline the process for collecting, analyzing, and sharing threat information.
- Records of threat intelligence received and shared with internal stakeholders and external partners.
- Analysis reports based on threat intelligence that inform security strategies and operations.
- Training records for security analysts on threat intelligence tools and analysis techniques.
- Membership or participation records in threat intelligence sharing platforms or industry groups.

DE.AE-07.02: Relevant event data is packaged for subsequent review and triage and events are categorized for efficient handling, assignment, and escalation.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #forensics | #incident_management | #root_cause_analysis

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Organizations should collect and package event data from multiple sources and sensors for efficient handling, assignment, and escalation. Describe capabilities in place to collect, analyze, and correlate events data. For example, a security information and event management (SIEM) tool can be used to aggregate event data for analysis and correlation. Describe how the organization performs timely collection of relevant event data, and automated analysis (IDS, IPS). Describe the tools used for event data collection.

Provide information on how relevant event data is packaged into subsequent review and triage. Describe how the identified events are categorized. Describe related policies, standards, procedures, or standardized event reporting templates in place. Describe escalation procedures for event data.

Examples of Effective Evidence:

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-081: Incident Analysis and Triage Process Documentation

- Documentation of standardized processes for analyzing and triaging security incidents, including criteria for categprization and prioritization.
- Logs and reports from incident management systems showing the application of triage processes in real incidents.
- After-action reviews or lessons learned documents from incidents, highlighting the effectiveness of analysis and triage procedures.
- Continuous improvement plans based on feedback and performance metrics from incident analysis activities.

DETECT / Adverse Event Analysis / Incident Declaration

DE.AE-08.01: Defined criteria and severity levels are in place to facilitate the declaration, escalation, organization, and alignment of response activities to response plans within the organization and across relevant third parties.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #incident_management | #information_sharing

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Incident response plans should include defined criteria and severity levels and processes to assign severity ratings to an incident. Organizations should establish criteria and severity levels to prioritize incidents and provide a timely response. Response activities should be in alignment of defined criteria, severity levels and escalation protocols.

Describe incident response policies and plans in place that outline the declaration, escalation, organization, and alignment of response activities within the organization and across relevant third parties. Provide information on how the organization's incident response plan describes how to appropriately document and report cyber events and related incident response activities. Describe how severity levels facilitate response activities to allow for a more effective incident response.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

RESPOND / Incident Management / Response Plan Execution

RS.MA-01.01: The organization's response plans are in place and executed during or after an incident, to include coordination with relevant third parties and engagement of third-party incident support services.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #forensics | #incident_management | #root_cause_analysis

Response Guidance:

The organization should have incident response policies and plans that properly work in concert with business continuity plans and should execute such plans during or after identifying an incident.

Responses should describe how the organization's response plans are established, maintained, and executed during or after an incident, including coordination with relevant third parties and engagement of third-party incident support services. Provide information on the structure and process.

Refer to ID.IM-04.08, how the organization's response plans are updated and improved based on cyber threat intelligence and lessons learned.

Examples of Effective Evidence:

EEE-070: Incident Management and Forensic Training Documents

- Curricula and materials for training programs focused on incident management and forensic investigation techniques.
- Attendance and completion records for employees who have undergone incident management and forensic training.
- Certifications or qualifications obtained by staff in incident management and forensic analysis disciplines.
- Summaries of training exercises, including objectives, scenarios, and participant performance evaluations.
- Feedback from training participants, used to continuously improve the training content and delivery methods.

EEE-088: Incident Management Role and Training Documentation

- Role definitions and responsibilities for incident management team members, clearly documented and communicated.
- Training programs and records for individuals involved in incident management, covering their specific roles and responsibilities.
- Incident response exercises or simulations, including role-playing scenarios that reinforce role clarity and preparedness.
- Feedback and evaluation reports from incident management activities, assessing role performance and identifying training needs.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Organizational charts or matrices that visually represent the incident management structure and roles.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

RESPOND / Incident Management / Incident Triage & Validation

RS.MA-02.01: Tools and processes are in place to ensure timely detection, inspection, assessment, and analysis of security event data for reliable activation of incident response processes.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #incident_management | #security_logging_monitoring_and_alerting

Response Guidance:

The most effective way to detect and prevent network compromise and data breaches is through early recognition and investigation of potentially suspicious network activity. The organization may use active and/or passive monitoring tools and processes to detect any deviations from normal or expected operations (i.e., network-monitoring software, logging, detection solutions, etc.).

Responses should describe the tools and processes that are in place to ensure timely detection, inspection, assessment, and analysis of the security event data for reliable activation of incident response processes.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

RESPOND / Incident Management / Incident Categorization & Prioritization

RS.MA-03.01: The organization categorizes and prioritizes cybersecurity incident response consistent with response plans and criticality of systems and services to the enterprise.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #critical_infrastructure | #incident_management | #risk_management

Response Guidance:

The incident response plan should include appropriate steps for assessing the root cause of the incident, and whether it includes appropriate guidance for performing analysis and for determining management's actions and operational steps that would minimize the relative impact of the incident on the organization's systems, information, and business. The incident response plan should be designed to prioritize incidents, enabling a rapid response for significant cybersecurity incidents or vulnerabilities.

Describe how cybersecurity incident response is categorized and prioritized, and how the categorization and prioritization is consistent with response plans and criticality of systems to the enterprise. Describe the timing expectations for incident response and the process for downgrading incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

RESPOND / Incident Management / Incident Escalation

RS.MA-04.01: Response activities are centrally coordinated, response progress and milestones are tracked and documented, and new incident information is assimilated into ongoing tasks, assignments, and escalations.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #incident_management | #information_sharing | #roles_and_responsibilities

Response Guidance:

The organization's incident response plan should appropriately document incident response activities. Response activities should be in alignment of defined criteria and severity levels. Describe incident response policies and plans in place that outline the declaration, escalation, organization, and alignment of response activities within the organization and across relevant third parties.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Describe how the response activities are centrally coordinated. Provide information on how response progress and milestones are tracked and document. Describe how new incident information is assimilated into ongoing tasks, assignments, and escalations.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

RESPOND / Incident Management / Recovery Initiation

RS.MA-05.01: The organization's incident response plans define severity levels and associated criteria for initiating response plans and escalating event response to appropriate stakeholders and management levels.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #incident_management | #information_sharing | #roles_and_responsibilities

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

The incident response plans should include related information on the incident's severity levels, and communications plans. The response plans should operate with the authority to collect and document information on the incident, assess risk, implement mitigation strategies, escalate issues when necessary, and consider any necessary changes to business practices.

Provide information on how the organization's incident response plan defines severity levels and associated criteria for initiating response plans. Describe reporting and escalation processes to the appropriate stakeholders and management levels.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

RESPOND / Incident Analysis / Incident Analysis & Root Cause Determination

RS.AN-03.01: The organization performs a thorough investigation to determine the nature and scope of an event, possible root causes, and the potential damage inflicted.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #forensics | #incident_management | #lessons_learned | #root_cause_analysis

Response Guidance:

The organization should review the impact of the cybersecurity incident, as analyzing the impact helps organizations align and prioritize resources to risks.

Describe how the organization performs thorough investigations in order to determine the nature and scope of an event, possible root causes, and the potential damage inflicted. Provide information on any functional teams in place and their roles and responsibilities. Functional teams may include forensics and root cause analysis teams, among others.

Examples of Effective Evidence:

EEE-028: Investigation and Forensic Documentation

- Standard operating procedures (SOPs) for conducting security investigations and handling forensic data.
- Chain of custody forms and logs that track the handling and analysis of forensic evidence.
- Forensic toolkits and software licenses used for data analysis during investigations.
- Forensic investigation reports detailing the rigor of methods applied.
- Training certifications and other qualifications for personnel or third parties involved in forensic investigations.
- Reports from completed investigations, including methodologies, findings, and recommendations.

EEE-070: Incident Management and Forensic Training Documents

- Curricula and materials for training programs focused on incident management and forensic investigation techniques.
- Attendance and completion records for employees who have undergone incident management and forensic training.
- Certifications or qualifications obtained by staff in incident management and forensic analysis disciplines.
- Summaries of training exercises, including objectives, scenarios, and participant performance evaluations.
- Feedback from training participants, used to continuously improve the training content and delivery methods.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-081: Incident Analysis and Triage Process Documentation

- Documentation of standardized processes for analyzing and triaging security incidents, including criteria for categprization and prioritization.
- Logs and reports from incident management systems showing the application of triage processes in real incidents.
- After-action reviews or lessons learned documents from incidents, highlighting the effectiveness of analysis and triage procedures.
- Continuous improvement plans based on feedback and performance metrics from incident analysis activities.

EEE-082: Forensic Data Security and Impact Assessment Documentation

- Policies and procedures for conducting forensic analysis and assessing the impact of security incidents.
- Records of forensic analysis tools and software licenses, ensuring the availability of necessary resources.
- Documentation of completed forensic analyses, including methodologies, findings, and recommendations for preventing future incidents.
- Training certifications for personnel responsible for forensic analysis and impact assessments.
- Summaries of incident impact assessments presented to management, detailing the consequences and lessons learned.

EEE-088: Incident Management Role and Training Documentation

- Role definitions and responsibilities for incident management team members, clearly documented and communicated.
- Training programs and records for individuals involved in incident management, covering their specific roles and responsibilities.
- Incident response exercises or simulations, including role-playing scenarios that reinforce role clarity and preparedness.
- Feedback and evaluation reports from incident management activities, assessing role performance and identifying training needs.
- Organizational charts or matrices that visually represent the incident management structure and roles.

RESPOND / Incident Analysis / Investigation Documentation

RS.AN-06.01: The organization establishes a risk-based approach and procedures for quarantining systems, conducting investigations, and collecting and preserving evidence per best practices and forensic standards.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #forensics | #incident_management | #infrastructure_security | #network_segmentation | #risk_management | #root_cause_analysis

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Organizations should assist in or conduct forensic investigations of cybersecurity incidents. Describe the risk-based approach and procedures implemented for quarantining systems, conducting investigations, and collecting and preserving evidence. Provide information on how procedures are aligned to best practices and forensic standards. Provide information on the forensics function and processes related to investigations and engineering of protective and detective controls.

Organizations may outsource security investigations and forensic analysis to skilled and qualified third parties. If the organization outsources such investigations, it should have an appropriate due diligence process in place to ensure any third party is fully qualified to perform the services contracted.

Examples of Effective Evidence:

EEE-028: Investigation and Forensic Documentation

- Standard operating procedures (SOPs) for conducting security investigations and handling forensic data.
- Chain of custody forms and logs that track the handling and analysis of forensic evidence.
- Forensic toolkits and software licenses used for data analysis during investigations.
- Forensic investigation reports detailing the rigor of methods applied.
- Training certifications and other qualifications for personnel or third parties involved in forensic investigations.
- Reports from completed investigations, including methodologies, findings, and recommendations.

EEE-070: Incident Management and Forensic Training Documents

- Curricula and materials for training programs focused on incident management and forensic investigation techniques.
- Attendance and completion records for employees who have undergone incident management and forensic training.
- Certifications or qualifications obtained by staff in incident management and forensic analysis disciplines.
- Summaries of training exercises, including objectives, scenarios, and participant performance evaluations.
- Feedback from training participants, used to continuously improve the training content and delivery methods.

EEE-081: Incident Analysis and Triage Process Documentation

- Documentation of standardized processes for analyzing and triaging security incidents, including criteria for categprization and prioritization.
- Logs and reports from incident management systems showing the application of triage processes in real incidents.
- After-action reviews or lessons learned documents from incidents, highlighting the effectiveness of analysis and triage procedures.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Continuous improvement plans based on feedback and performance metrics from incident analysis activities.

EEE-082: Forensic Data Security and Impact Assessment Documentation

- Policies and procedures for conducting forensic analysis and assessing the impact of security incidents.
- Records of forensic analysis tools and software licenses, ensuring the availability of necessary resources.
- Documentation of completed forensic analyses, including methodologies, findings, and recommendations for preventing future incidents.
- Training certifications for personnel responsible for forensic analysis and impact assessments.
- Summaries of incident impact assessments presented to management, detailing the consequences and lessons learned.

RESPOND / Incident Analysis / Incident Data Collection & Preservation

RS.AN-07.01: Incident-related forensic data is captured, secured, and preserved in a manner supporting integrity, provenance, and evidentiary value.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #forensics | #incident_management | #root_cause_analysis

Response Guidance:

As referenced in RS.AN-03.01, the organization performs thorough investigations in order to determine the nature of a cyber-event, its extent, and the damage inflicted. Forensic analysis should be performed by qualified staff or third parties. Describe how incident-related forensic data is captured, secured, and preserved in a manner supporting integrity, provenance, and evidentiary value. Provide information of policies, standards, and procedures established to achieve this requirement.

Provide information on any functional teams in place and their roles and responsibilities. Functional teams may include forensics and root cause analysis teams, among others.

Examples of Effective Evidence:

EEE-028: Investigation and Forensic Documentation

- Standard operating procedures (SOPs) for conducting security investigations and handling forensic data.
- Chain of custody forms and logs that track the handling and analysis of forensic evidence.
- Forensic toolkits and software licenses used for data analysis during investigations.
- Forensic investigation reports detailing the rigor of methods applied.
- Training certifications and other qualifications for personnel or third parties involved in forensic investigations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Reports from completed investigations, including methodologies, findings, and recommendations.

EEE-070: Incident Management and Forensic Training Documents

- Curricula and materials for training programs focused on incident management and forensic investigation techniques.
- Attendance and completion records for employees who have undergone incident management and forensic training.
- Certifications or qualifications obtained by staff in incident management and forensic analysis disciplines.
- Summaries of training exercises, including objectives, scenarios, and participant performance evaluations.
- Feedback from training participants, used to continuously improve the training content and delivery methods.

EEE-081: Incident Analysis and Triage Process Documentation

- Documentation of standardized processes for analyzing and triaging security incidents, including criteria for categprization and prioritization.
- Logs and reports from incident management systems showing the application of triage processes in real incidents.
- After-action reviews or lessons learned documents from incidents, highlighting the effectiveness of analysis and triage procedures.
- Continuous improvement plans based on feedback and performance metrics from incident analysis activities.

EEE-082: Forensic Data Security and Impact Assessment Documentation

- Policies and procedures for conducting forensic analysis and assessing the impact of security incidents.
- Records of forensic analysis tools and software licenses, ensuring the availability of necessary resources.
- Documentation of completed forensic analyses, including methodologies, findings, and recommendations for preventing future incidents.
- Training certifications for personnel responsible for forensic analysis and impact assessments.
- Summaries of incident impact assessments presented to management, detailing the consequences and lessons learned.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

RESPOND / Incident Analysis / Incident Magnitude Determination

RS.AN-08.01: Available incident information is assessed to determine the extent of impact to the organization and its stakeholders, the potential near- and long-term financial implications<font

color=black>, and whether or not the incident constitutes a material event.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #incident_management

Response Guidance:

Organizations should have policies, standards, and processes in place to assess the impact associated with cybersecurity incidents. As referenced in DE.AE-04.01, the impact should be determined based upon their nature, extent, potential magnitude, and the range of harm such incidents could cause to the organization's reputation, financial performance, customer relations, and impact across the financial sector.

The organization must determine if an incident constitutes a material event to the company and its stakeholders, which has regularly reporting implications. Such determinations should be made at the most senior levels of a company, and with the advice of legal counsel and the Chief Information Security Office. Describe how available incident information is assessed to determine the extent of impact to the organization and its stakeholders, the potential near- and long-term financial implications, and the determination of incident materiality.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-028: Investigation and Forensic Documentation

- Standard operating procedures (SOPs) for conducting security investigations and handling forensic data.
- Chain of custody forms and logs that track the handling and analysis of forensic evidence.
- Forensic toolkits and software licenses used for data analysis during investigations.
- Forensic investigation reports detailing the rigor of methods applied.
- Training certifications and other qualifications for personnel or third parties involved in forensic investigations.
- Reports from completed investigations, including methodologies, findings, and recommendations.

EEE-070: Incident Management and Forensic Training Documents

- Curricula and materials for training programs focused on incident management and forensic investigation techniques.
- Attendance and completion records for employees who have undergone incident management and forensic training.
- Certifications or qualifications obtained by staff in incident management and forensic analysis disciplines.
- Summaries of training exercises, including objectives, scenarios, and participant performance evaluations.
- Feedback from training participants, used to continuously improve the training content and delivery methods.

RESPOND / Incident Response Reporting and Communication / Stakeholder Incident Notification

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

RS.CO-02.01: The organization's incident response program includes defined and approved escalation protocols, linked to organizational decision levels and communication strategies, including which types of information will be shared, with whom (e.g., the organization's governing authority and senior management), and how information provided to the organization will be acted upon.

Subject Tags: #incident_management | #information_sharing | #roles_and_responsibilities

Response Guidance:

The organization’s incident response plan should specify which incidents must be reported, when they must be reported, and to whom based on the severity level of the incident. Parties commonly notified of cyber incidents include the CIO, head of information security, local information security officer, legal counsel, other incident response teams, and system owners, among others.

Describe how the organization's incident response program includes defined and approved escalation protocols, linked to organizational decision levels and communication strategies, including which types of information will be shared, with whom (e.g., the organization's appropriate governing

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

authority and senior management), and how information provided to the organization will be acted upon. Focus evidence on escalation protocols and related processes, based on the severity level of the incident.

Examples of Effective Evidence:

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-083: Incident Escalation and Communication Protocol Documentation

- Escalation procedures that outline the steps for escalating incidents within the organization, including roles and responsibilities.
- Templates, protocols, and automated tool configurations for internal and external communication during and after security incidents.
- Identified fail-over communication methods.
- Records of incident response exercises testing the escalation and communication processes.
- Incident logs demonstrating the application of escalation and communication protocols in actual incidents.
- Feedback from stakeholders on the effectiveness and clarity of communications during incident response.

EEE-088: Incident Management Role and Training Documentation

- Role definitions and responsibilities for incident management team members, clearly documented and communicated.
- Training programs and records for individuals involved in incident management, covering their specific roles and responsibilities.
- Incident response exercises or simulations, including role-playing scenarios that reinforce role clarity and preparedness.
- Feedback and evaluation reports from incident management activities, assessing role performance and identifying training needs.
- Organizational charts or matrices that visually represent the incident management structure and roles.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

RS.CO-02.02: In the event of an incident, the organization notifies impacted stakeholders including, as required, government bodies, self-regulatory agencies and/or other supervisory bodies, within required timeframes.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #incident_management | #information_sharing | #roles_and_responsibilities

Response Guidance:

The incident response program should include reporting procedures to ensure that the organization promptly reports incident information to appropriate authorities, such as primary regulators and law enforcement. The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, directives, policies, regulations, standards and guidance.

Describe the process the organization utilizes to notify impacted stakeholders including, as required, government bodies, self-regulatory agencies or any other supervisory bodies in the event of an incident. Provide information with a focus on stakeholders. If an incident is determined to be a material event, in the U.S., required SEC regulatory filings must be made. Describe how the organization notifies impacted stakeholders within required timeframes.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-060: Cross-Sector Incident Response Coordination Documents

- Coordination plans that outline how the organization will work with external entities during an incident response.
- Agreements or MOUs with cross-sector partners and government agencies for collaborative information sharing and/orincident response.
- After-action reports from joint incident response exercises with cross-sector partners.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Communication protocols for sharing information and coordinating actions during cross-sector incidents.
- Training and exercise records for staff on cross-sector incident response procedures.

EEE-083: Incident Escalation and Communication Protocol Documentation

- Escalation procedures that outline the steps for escalating incidents within the organization, including roles and responsibilities.
- Templates, protocols, and automated tool configurations for internal and external communication during and after security incidents.
- Identified fail-over communication methods.
- Records of incident response exercises testing the escalation and communication processes.
- Incident logs demonstrating the application of escalation and communication protocols in actual incidents.
- Feedback from stakeholders on the effectiveness and clarity of communications during incident response.

EEE-084: Cyber Threat Intelligence Sharing and Distribution Documents

- Policies and procedures for collecting, analyzing, and distributing cyber threat intelligence within the organization and with external partners.
- Agreements or memberships with threat intelligence sharing platforms or industry groups.
- Records of threat intelligence briefings or alerts issued to relevant stakeholders.
- Evaluations of the threat intelligence program, assessing its contribution to the organization's security posture.

EEE-101: Cyber Threat Intelligence Sharing Documentation

- Cyber threat intelligence policies that outline the process for collecting, analyzing, and sharing threat information.
- Records of threat intelligence received and shared with internal stakeholders and external partners.
- Analysis reports based on threat intelligence that inform security strategies and operations.
- Training records for security analysts on threat intelligence tools and analysis techniques.
- Membership or participation records in threat intelligence sharing platforms or industry groups.

RS.CO-02.03: The organization maintains and regularly tests incident response communication procedures, with associated contact lists, call trees, and automatic notifications, to quickly coordinate and communicate with internal and external stakeholders during or following an incident.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #incident_management | #information_sharing | #review_assessment_and_testing

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

The organization should have policies and procedures for communicating cyber and operational incidents to internal and external stakeholders. Internal communication can occur through various methods, including communicational channels, building out contact lists, automatic notifications, among others. Testing should be performed on incident response communication procedures to ensure timely response of incidents.

Describe testing regularly performed on incident response communication procedures to quickly coordinate and communicate with internal and external stakeholders during or following an incident. Provide information on the communications plan activities (e.g., associated contact lists, call trees, and automated notification tools).

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-044: Security Incident and Event Management Documentation

- Written policies outlining the procedures for managing security incidents and events, including roles and responsibilities.
- Configuration and operational guidelines for Security Information and Event Management (SIEM) systems.
- Logs and analysis reports from the SIEM system, demonstrating the detection and handling of security events.
- Training documentation for personnel responsible for managing the SIEM system and responding to incidents.
- Audit trails and incident reports that document the response to and resolution of security incidents.

EEE-083: Incident Escalation and Communication Protocol Documentation

- Escalation procedures that outline the steps for escalating incidents within the organization, including roles and responsibilities.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Templates, protocols, and automated tool configurations for internal and external communication during and after security incidents.
- Identified fail-over communication methods.
- Records of incident response exercises testing the escalation and communication processes.
- Incident logs demonstrating the application of escalation and communication protocols in actual incidents.
- Feedback from stakeholders on the effectiveness and clarity of communications during incident response.

RESPOND / Incident Response Reporting and Communication / Stakeholder Incident Information Sharing

RS.CO-03.01: The organization ensures that cyber threat intelligence is made available, in a secure manner, to authorized staff with responsibility for the mitigation of cyber risks at the strategic, tactical and operational levels within the organization.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #information_sharing | #threat_management

Response Guidance:

Threat intelligence information should be collected and analyzed for dissemination to appropriate individuals for action. When establishing and reviewing information sharing rules, the organization should request input from legal and privacy officials, information owners, management, and other key stakeholders to ensure that cyber threat intelligence information is being shared in accordance with the organization's policies and procedures.

Describe how the organization ensures that cyber threat intelligence, which may include cyber incident information and sensitive organizational data as appropriate, is made available, in a secure manner, to authorized staff with responsibility for the mitigation of cyber risks at the strategic, tactical, and operational levels within the organization. Describe the roles and responsibilities related to the distribution of cyber threat intelligence.

Examples of Effective Evidence:

EEE-084: Cyber Threat Intelligence Sharing and Distribution Documents

- Policies and procedures for collecting, analyzing, and distributing cyber threat intelligence within the organization and with external partners.
- Agreements or memberships with threat intelligence sharing platforms or industry groups.
- Records of threat intelligence briefings or alerts issued to relevant stakeholders.
- Evaluations of the threat intelligence program, assessing its contribution to the organization's security posture.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-101: Cyber Threat Intelligence Sharing Documentation

- Cyber threat intelligence policies that outline the process for collecting, analyzing, and sharing threat information.
- Records of threat intelligence received and shared with internal stakeholders and external partners.
- Analysis reports based on threat intelligence that inform security strategies and operations.
- Training records for security analysts on threat intelligence tools and analysis techniques.
- Membership or participation records in threat intelligence sharing platforms or industry groups.

RS.CO-03.02: In the event of an incident, the organization shares authorized information, in a defined manner and through trusted channels, to facilitate the detection, response, resumption and recovery of its own systems and those of other partners and critical sector participants.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #disaster_recovery | #incident_management | #information_sharing

Response Guidance:

The organization should actively participate in information sharing organizations (i.e., the Analysis and Resilience Center for Systemic Risk (ARC), FS-ISAC, industry associations) to receive and provide external threat and vulnerability information. The organization can also establish threat intelligence sharing relationships directly with peer organizations. To protect the confidentiality and the integrity of the information, organizations should have formal information sharing agreements that document the nature of the information being shared, handling and storage, ownership, retention, and related matters.

Describe how the organization actively participates in multilateral information-sharing arrangements to facilitate a sector-wide response to large-scale incidents. Provide information related to the sector-wide information sharing.

Describe how information is shared consistent with response plans. Describe how the organization shares authorized information, in a defined manner and through trusted channels, to facilitate the detection, response, resumption and recovery of its own systems and those of other partners and critical sector participants.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-084: Cyber Threat Intelligence Sharing and Distribution Documents

- Policies and procedures for collecting, analyzing, and distributing cyber threat intelligence within the organization and with external partners.
- Agreements or memberships with threat intelligence sharing platforms or industry groups.
- Records of threat intelligence briefings or alerts issued to relevant stakeholders.
- Evaluations of the threat intelligence program, assessing its contribution to the organization's security posture.

EEE-101: Cyber Threat Intelligence Sharing Documentation

- Cyber threat intelligence policies that outline the process for collecting, analyzing, and sharing threat information.
- Records of threat intelligence received and shared with internal stakeholders and external partners.
- Analysis reports based on threat intelligence that inform security strategies and operations.
- Training records for security analysts on threat intelligence tools and analysis techniques.
- Membership or participation records in threat intelligence sharing platforms or industry groups.

EEE-106: Recovery Objectives Critical Infrastructure Documentation

- Documentation of recovery objectives for critical infrastructure and how these align with business continuity goals.
- Critical infrastructure analysis reports that assess the resilience and recovery capabilities of essential systems.
- Records of alignment discussions or decisions between recovery objectives and business needs.
- Audit reports evaluating the alignment of recovery objectives with the criticality of infrastructure components.

EEE-107: Data Recovery and Information Flow Mapping Documentation

- Data recovery strategy documents that outline procedures for restoring lost or corrupted data.
- Information flow maps that illustrate how data moves through the organization, informing recovery planning.
- Test reports from data recovery exercises, demonstrating the ability to restore data in line with recovery strategies.
- Documentation of changes to data recovery strategies based on new business processes or technologies.
- Training records for IT staff on data recovery procedures and information flow considerations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

RESPOND / Incident Mitigation / Incident Containment

RS.MI-01.01: The organization has established processes to implement vulnerability mitigation plans, involve third-party partners and outside expertise as needed, and contain incidents in a timely manner.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #incident_management | #staffing_and_resource_management | #vulnerability_management

Response Guidance:

Describe the established processes to implement vulnerability mitigation plans, as well as validate their completion and effectiveness. Describe how the organization mitigates cybersecurity incidents in a timely manner. Provide examples.

Provide information on how mitigation plans are reviewed and agreed upon with business stakeholders. Provide information on how remediation is tested and verified.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.
- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.
- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

RESPOND / Incident Mitigation / Incident Eradication

RS.MI-02.01: Targeted investigations and actions are taken to ensure that all vulnerabilities, system components, devices, or remnants used or leveraged in an attack (e.g., malware, compromised accounts, open ports, etc.) are removed or otherwise returned to a secure and reliable state, or that plans to address the vulnerabilities are documented.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #endpoint_security | #incident_management | #infrastructure_security | #lessons_learned | #root_cause_analysis | #vulnerability_management

Response Guidance:

Organizations should have strategies and procedures for mitigation and eradication in place for a timely containment of vulnerabilities. Describe eradication processes in place. Describe how targeted investigations determine root causes of incidents and provide actionable results to ensure that all vulnerabilities are removed or otherwise returned to a secure and reliable state.

Describe target investigations and actions taken to ensure that all vulnerabilities, system components, devices, or remnants used or leveraged in an action are removed or otherwise returned to a secure and reliable state. Provide information of documented plans to address the identified vulnerabilities.

Examples of Effective Evidence:

EEE-028: Investigation and Forensic Documentation

- Standard operating procedures (SOPs) for conducting security investigations and handling forensic data.
- Chain of custody forms and logs that track the handling and analysis of forensic evidence.
- Forensic toolkits and software licenses used for data analysis during investigations.
- Forensic investigation reports detailing the rigor of methods applied.
- Training certifications and other qualifications for personnel or third parties involved in forensic investigations.
- Reports from completed investigations, including methodologies, findings, and recommendations.

EEE-047: Vulnerability Management and Remediation Strategy Documentation

- Policies and procedures for identifying, assessing, and remediating vulnerabilities in systems and software.
- Vulnerability scan reports and dashboards showing identified vulnerabilities and their remediation status.
- Change management records for remediation actions taken in response to identified vulnerabilities.
- Documentation of prioritization criteria for addressing vulnerabilities based on risk.
- Records of communication with stakeholders regarding vulnerability management efforts and outcomes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-075: Malware and Mobile Code Defense Strategy Documents

- Policies and procedures for defending against malware and malicious mobile code, including prevention, detection, and response strategies.
- Configuration records for anti-malware tools and systems, showing protective measures in place.
- Logs and reports from anti-malware solutions, documenting detections and actions taken.
- Post-incident analysis documents that evaluate the response to malware incidents and the effectiveness of defense mechanisms.

RECOVER / Incident Recovery Plan Execution / Recovery Plan Execution

RC.RP-01.01: The organization executes its recovery plans, including incident recovery, disaster recovery, and business continuity plans, during or after an incident to resume operations.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #data_backup | #disaster_recovery | #hotswap | #incident_management | #resilience

Response Guidance:

The organization should have incident recovery, disaster recovery, business continuity, and data backup plans to recover operations following an incident.

Describe how the organization executes its recovery plans, including incident recovery, disaster recovery, and business continuity plans, during or after an incident to resume operations. Provide information on trigger event and/or criteria.

Examples of Effective Evidence:

EEE-061: Service Recovery and Critical Operations Resumption Documentation

- Procedures and checklists for resuming services and recovering critical operations after an incident.
- Prioritization lists that identify critical services and operations for recovery efforts.
- Test results and reports from service resumption drills and recovery exercises.
- Service level agreements (SLAs) with vendors that include provisions for rapid service resumption.
- Documentation of alternative processes and workarounds to be used when primary operations are disrupted.

EEE-078: Resilience Testing and Infrastructure Redundancy Documentation

- Documentation of resilience testing plans and procedures, including objectives, scenarios, and expected outcomes.
- Test reports summarizing the results of resilience testing exercises, highlighting strengths and areas for improvement.
- Infrastructure redundancy designs and implementation records, showing failover capabilities and backup systems.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Change management records documenting updates or enhancements made to improve infrastructure redundancy.
- Stakeholder feedback on the organization's resilience and redundancy capabilities, gathered after testing or actual events.

EEE-086: Recovery Strategy and Resilience Plan Documentation

- Documentation of the organization's recovery strategies, including plans for restoring critical services and operations after an incident.
- Change logs or records showing updates to recovery strategies and resilience plans based on lessons learned from exercises or actual incidents.
- Stakeholder feedback and review summaries that have led to updates in recovery strategies or resilience plans.
- Training session records for staff on updated recovery procedures and resilience measures.
- Audit reports or assessments that have identified areas for improvement in recovery strategies, leading to plan updates.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EEE-106: Recovery Objectives Critical Infrastructure Documentation

- Documentation of recovery objectives for critical infrastructure and how these align with business continuity goals.
- Critical infrastructure analysis reports that assess the resilience and recovery capabilities of essential systems.
- Records of alignment discussions or decisions between recovery objectives and business needs.
- Audit reports evaluating the alignment of recovery objectives with the criticality of infrastructure components.

EEE-107: Data Recovery and Information Flow Mapping Documentation

- Data recovery strategy documents that outline procedures for restoring lost or corrupted data.
- Information flow maps that illustrate how data moves through the organization, informing recovery planning.
- Test reports from data recovery exercises, demonstrating the ability to restore data in line with recovery strategies.
- Documentation of changes to data recovery strategies based on new business processes or technologies.
- Training records for IT staff on data recovery procedures and information flow considerations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

EEE-111: Disaster Recovery and Validation Program Documentation

- Disaster Recovery (DR) plans outlining specific recovery steps for Information Technology (IT) systems and data.
- Schedules and results from regular DR testing, ensuring plans are actionable and up-to-date.
- Change management records for DR plans, capturing updates and justifications.
- Records capturing lessons-learned from exercises and the updating of documentation and plans to reflect the improvements.
- Training and certification records for personnel on DR roles and procedures.
- Review reports assessing DR plan alignment with overall business recovery objectives and Business Impact Analyses (BIAs).

RECOVER / Incident Recovery Plan Execution / Recovery Action Performance

RC.RP-02.01: The organization's response plans are used as informed guidance to develop and manage task plans, response actions, priorities, and assignments for responding to incidents, but are adapted as necessary to address incident-specific characteristics.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #critical_infrastructure | #disaster_recovery | #incident_management | #resilience

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Incident response plans should outline the steps to execute an incident from preparation, detection and analysis, containment, eradication, and recovery. Describe how the organization's response plan is used as informed guidance to develop and manage incident-specific task plans and response activities. Describe how response activities are prioritized in accordance with the organization's response plans. Provide information of defined roles, responsibilities, and assignments for responding to incidents. Provide information on how plans, actions, priorities, and assignments are adapted as necessary to address incident-specific characteristics.

Examples of Effective Evidence:

EEE-078: Resilience Testing and Infrastructure Redundancy Documentation

- Documentation of resilience testing plans and procedures, including objectives, scenarios, and expected outcomes.
- Test reports summarizing the results of resilience testing exercises, highlighting strengths and areas for improvement.
- Infrastructure redundancy designs and implementation records, showing failover capabilities and backup systems.
- Change management records documenting updates or enhancements made to improve infrastructure redundancy.
- Stakeholder feedback on the organization's resilience and redundancy capabilities, gathered after testing or actual events.

EEE-086: Recovery Strategy and Resilience Plan Documentation

- Documentation of the organization's recovery strategies, including plans for restoring critical services and operations after an incident.
- Change logs or records showing updates to recovery strategies and resilience plans based on lessons learned from exercises or actual incidents.
- Stakeholder feedback and review summaries that have led to updates in recovery strategies or resilience plans.
- Training session records for staff on updated recovery procedures and resilience measures.
- Audit reports or assessments that have identified areas for improvement in recovery strategies, leading to plan updates.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

RC.RP-02.02: Recovery plans are executed by first resuming critical services and core business functions, while minimizing any potential concurrent and widespread interruptions to interconnected entities and critical infrastructure, such as energy and telecommunications.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #asset_inventory | #asset_management | #business_impact_analysis | #critical_infrastructure | #disaster_recovery | #resilience | #review_assessment_and_testing | #risk_management | #threat_landscape

Response Guidance:

A formal backup and recovery plan describes how critical systems are backed up and restored in the event of loss or corruption of production data. The organization should have a process in place to conduct business impact analysis to identify criticality.

Describe how recovery plans are executed by first resuming critical services and core business functions within a defined timeframe. Describe how the plans could be executed while minimizing any potential concurrent and widespread interruptions to interconnected entities and critical infrastructure, such as energy and telecommunications (e.g., how recovery plans include communication plans with interconnected entities).

Examples of Effective Evidence:

EEE-086: Recovery Strategy and Resilience Plan Documentation

- Documentation of the organization's recovery strategies, including plans for restoring critical services and operations after an incident.
- Change logs or records showing updates to recovery strategies and resilience plans based on lessons learned from exercises or actual incidents.
- Stakeholder feedback and review summaries that have led to updates in recovery strategies or resilience plans.
- Training session records for staff on updated recovery procedures and resilience measures.
- Audit reports or assessments that have identified areas for improvement in recovery strategies, leading to plan updates.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-106: Recovery Objectives Critical Infrastructure Documentation

- Documentation of recovery objectives for critical infrastructure and how these align with business continuity goals.
- Critical infrastructure analysis reports that assess the resilience and recovery capabilities of essential systems.
- Records of alignment discussions or decisions between recovery objectives and business needs.
- Audit reports evaluating the alignment of recovery objectives with the criticality of infrastructure components.

EEE-107: Data Recovery and Information Flow Mapping Documentation

- Data recovery strategy documents that outline procedures for restoring lost or corrupted data.
- Information flow maps that illustrate how data moves through the organization, informing recovery planning.
- Test reports from data recovery exercises, demonstrating the ability to restore data in line with recovery strategies.
- Documentation of changes to data recovery strategies based on new business processes or technologies.
- Training records for IT staff on data recovery procedures and information flow considerations.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

EEE-111: Disaster Recovery and Validation Program Documentation

- Disaster Recovery (DR) plans outlining specific recovery steps for Information Technology (IT) systems and data.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Schedules and results from regular DR testing, ensuring plans are actionable and up-to-date.
- Change management records for DR plans, capturing updates and justifications.
- Records capturing lessons-learned from exercises and the updating of documentation and plans to reflect the improvements.
- Training and certification records for personnel on DR roles and procedures.
- Review reports assessing DR plan alignment with overall business recovery objectives and Business Impact Analyses (BIAs).

RECOVER / Incident Recovery Plan Execution / Backup & Restoration Asset Integrity

RC.RP-03.01: Restoration steps include the verification of backups, data replications, system images, and other restoration assets prior to continued use.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #data_backup | #disaster_recovery | #resilience

Response Guidance:

Organizations should have processes to validate recovery capabilities to ensure that tools, technologies, and recovery processes are effective in the resumption of critical operations.

Describe how the organization verifies backups, data replications, system images, and other restoration assets prior to continued use. Provide information of restoration steps in place to restore assets and ensure they are fully functional.

Examples of Effective Evidence:

EEE-086: Recovery Strategy and Resilience Plan Documentation

- Documentation of the organization's recovery strategies, including plans for restoring critical services and operations after an incident.
- Change logs or records showing updates to recovery strategies and resilience plans based on lessons learned from exercises or actual incidents.
- Stakeholder feedback and review summaries that have led to updates in recovery strategies or resilience plans.
- Training session records for staff on updated recovery procedures and resilience measures.
- Audit reports or assessments that have identified areas for improvement in recovery strategies, leading to plan updates.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

RECOVER / Incident Recovery Plan Execution / Post-Incident Operational Norms

RC.RP-04.01: Restoration steps include the verification of data integrity, transaction positions, system functionality, and the operation of security controls by appropriate organizational stakeholders and system owners.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #data_backup | #disaster_recovery | #resilience

Response Guidance:

Organizations should have processes to validate recovery capabilities and ensure that tools, technologies, recovery processes, and people are effective in the resumption of critical operations.

Describe how the organization verifies data integrity, transaction positions, and system functionality. Describe how the organization verifies the operation of security controls by appropriate organizational stakeholders and system owners. Provide information of restoration steps in place to resume operational norms.

Examples of Effective Evidence:

EEE-061: Service Recovery and Critical Operations Resumption Documentation

- Procedures and checklists for resuming services and recovering critical operations after an incident.
- Prioritization lists that identify critical services and operations for recovery efforts.
- Test results and reports from service resumption drills and recovery exercises.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Service level agreements (SLAs) with vendors that include provisions for rapid service resumption.
- Documentation of alternative processes and workarounds to be used when primary operations are disrupted.

EEE-078: Resilience Testing and Infrastructure Redundancy Documentation

- Documentation of resilience testing plans and procedures, including objectives, scenarios, and expected outcomes.
- Test reports summarizing the results of resilience testing exercises, highlighting strengths and areas for improvement.
- Infrastructure redundancy designs and implementation records, showing failover capabilities and backup systems.
- Change management records documenting updates or enhancements made to improve infrastructure redundancy.
- Stakeholder feedback on the organization's resilience and redundancy capabilities, gathered after testing or actual events.

EEE-086: Recovery Strategy and Resilience Plan Documentation

- Documentation of the organization's recovery strategies, including plans for restoring critical services and operations after an incident.
- Change logs or records showing updates to recovery strategies and resilience plans based on lessons learned from exercises or actual incidents.
- Stakeholder feedback and review summaries that have led to updates in recovery strategies or resilience plans.
- Training session records for staff on updated recovery procedures and resilience measures.
- Audit reports or assessments that have identified areas for improvement in recovery strategies, leading to plan updates.

EEE-089: System Sanitization and Restoration Documents

- Procedures for the sanitization of systems and data to remove sensitive information securely before disposal or repurposing.
- Restoration procedures detailing steps to return systems to operational status after an incident or maintenance.
- Records of system sanitization and restoration activities, including dates, systems involved, and personnel responsible.
- Training records for IT staff on proper sanitization techniques and restoration protocols.
- Compliance reports or certifications demonstrating adherence to industry standards for data sanitization and system restoration.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

RECOVER / Incident Recovery Plan Execution / Asset Integrity Restoration

RC.RP-05.01: The organization maintains documented procedures for sanitizing, testing, authorizing, and returning systems to service following an incident or investigation.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #asset_management | #incident_management

Response Guidance:

Following an incident or investigation, an organization should have business continuity, recovery and/or resilience procedures in place to return systems to operational states. Provide information on procedures in place for sanitizing, testing, authorizing, and returning systems to service. For example, removing malicious code, and reimaging affected systems that were exploited. Restoration of systems should be done within defined recovery time and recovery point objectives for critical systems.

Examples of Effective Evidence:

EEE-028: Investigation and Forensic Documentation

- Standard operating procedures (SOPs) for conducting security investigations and handling forensic data.
- Chain of custody forms and logs that track the handling and analysis of forensic evidence.
- Forensic toolkits and software licenses used for data analysis during investigations.
- Forensic investigation reports detailing the rigor of methods applied.
- Training certifications and other qualifications for personnel or third parties involved in forensic investigations.
- Reports from completed investigations, including methodologies, findings, and recommendations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-089: System Sanitization and Restoration Documents

- Procedures for the sanitization of systems and data to remove sensitive information securely before disposal or repurposing.
- Restoration procedures detailing steps to return systems to operational status after an incident or maintenance.
- Records of system sanitization and restoration activities, including dates, systems involved, and personnel responsible.
- Training records for IT staff on proper sanitization techniques and restoration protocols.
- Compliance reports or certifications demonstrating adherence to industry standards for data sanitization and system restoration.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EEE-110: Data Recovery and Integrity Assurance Documentation

- Data recovery plans that describe the procedures for restoring critical data and systems after an incident, including roles and responsibilities.
- Policies and procedures for regular data integrity checks, ensuring the accuracy and completeness of data both under normal operations and during recovery.
- Documentation of backup and restoration procedures, including backup schedules, data retention policies, and the scope of backup data.
- Logs and reports from data integrity and recovery tests, demonstrating successful restoration and validation of data against integrity standards.
- Checklists, tools, and software used for conducting data integrity checks and for verifying successful data recovery during planned exercises or in response to actual incidents.
- Service level agreements (SLAs) with third-party vendors that outline responsibilities and expectations for data recovery services, including timeframes for restoration and data integrity guarantees.
- Training materials and records for IT staff and relevant personnel on data recovery and integrity maintenance procedures, including any certifications or acknowledgments of training completion.
- Audit reports or reviews that assess the organization's data recovery and integrity assurance practices, including any findings and subsequent corrective actions taken to improve data management.
- After-action reports and lessons learned from recovery exercises or actual data loss incidents, used to refine and improve recovery strategies and integrity verification processes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

RC.RP-05.02: Business, technology, cybersecurity, and relevant third-party stakeholders confirm that systems, data, and services have been returned to functional and secure states and that a stable operational status has been achieved.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #asset_management | #data_protection | #disaster_recovery | #incident_management | #third_party_risk_management | #supply_chain_management

Response Guidance:

Organizations should restore systems, data, and services to normal operations following an investigation or incident and verify that they have been returned to functional and secure states.

Provide information on the involvement of business, technology, cybersecurity, and relevant third-party stakeholders to confirm that systems, data, and services have returned to a stable and secure operational status. Describe recovery processes, policies, and procedures with focus on stakeholder involvement to achieve operational states.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-089: System Sanitization and Restoration Documents

- Procedures for the sanitization of systems and data to remove sensitive information securely before disposal or repurposing.
- Restoration procedures detailing steps to return systems to operational status after an incident or maintenance.
- Records of system sanitization and restoration activities, including dates, systems involved, and personnel responsible.
- Training records for IT staff on proper sanitization techniques and restoration protocols.
- Compliance reports or certifications demonstrating adherence to industry standards for data sanitization and system restoration.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EEE-111: Disaster Recovery and Validation Program Documentation

- Disaster Recovery (DR) plans outlining specific recovery steps for Information Technology (IT) systems and data.
- Schedules and results from regular DR testing, ensuring plans are actionable and up-to-date.
- Change management records for DR plans, capturing updates and justifications.
- Records capturing lessons-learned from exercises and the updating of documentation and plans to reflect the improvements.
- Training and certification records for personnel on DR roles and procedures.
- Review reports assessing DR plan alignment with overall business recovery objectives and Business Impact Analyses (BIAs).

RECOVER / Incident Recovery Plan Execution / End-of-Incident Determination

RC.RP-06.01: Incident management activities are closed under defined conditions and documentation to support subsequent post-mortem review, process improvement, and any follow-on activities is collected and verified.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #forensics | #incident_management | #lessons_learned | #root_cause_analysis

Response Guidance:

Organizations should have processes for post-incident analysis to evaluate the incident response process, discuss identified gaps, minimize future impact, and discuss the closure of the relevant incident. Provide information on applicable internal and external stakeholders involved.

Provide information on how the organization's establishes defined conditions and documentation to provide closure of incident management activities. Provide information of the subsequent post-mortem review. Describe how the post-incident process drives process improvements and incorporate lessons learned. Describe how the organization collects and verifies any follow-on activities needed for the closure of incident management activities.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-028: Investigation and Forensic Documentation

- Standard operating procedures (SOPs) for conducting security investigations and handling forensic data.
- Chain of custody forms and logs that track the handling and analysis of forensic evidence.
- Forensic toolkits and software licenses used for data analysis during investigations.
- Forensic investigation reports detailing the rigor of methods applied.
- Training certifications and other qualifications for personnel or third parties involved in forensic investigations.
- Reports from completed investigations, including methodologies, findings, and recommendations.

RECOVER / Incident Recovery Communication / Recovery Activity Communication

RC.CO-03.01: The organization timely involves and communicates the recovery activities, procedures, cyber risk management issues to the governing body (e.g., the Board or one of its committees), senior management, incident management support teams, and relevant internal stakeholders.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #board_or_committee_oversight | #disaster_recovery | #incident_management | #information_sharing | #risk_management

Response Guidance:

Describe how the organization timely involves and communicates the recovery activities, procedures, and cyber risk management issues to the appropriate governing body (e.g., the Board or one of its

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

committees), senior management, incident management support teams, and relevant internal stakeholders.

Examples of Effective Evidence:

EEE-022: Incident Management, Response Framework and Performance Documentation

- Integrated incident management policies and Incident Response Plan (IRP) that outline procedures for detecting, responding to, and recovering from security incidents, from detection to resolution.
- Configuration guides for SIEM systems and other detection tools, paired with response protocols.
- Combined logs of incident detection, analysis, and response activities, showing the full incident lifecycle.
- Training records and modules for the incident response team and security personnel, including exercises, simulations, and end-to-end incident management process.
- After-action reports, summaries, and lessons learned from incident response exercises, including key takeaways and action items.
- Metrics and performance indicators that track the effectiveness of the incident response program.
- Audit reports evaluating the effectiveness of the incident management framework and suggesting improvements.

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-106: Recovery Objectives Critical Infrastructure Documentation

- Documentation of recovery objectives for critical infrastructure and how these align with business continuity goals.
- Critical infrastructure analysis reports that assess the resilience and recovery capabilities of essential systems.
- Records of alignment discussions or decisions between recovery objectives and business needs.
- Audit reports evaluating the alignment of recovery objectives with the criticality of infrastructure components.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

RC.CO-03.02: The organization promptly communicates the status of recovery activities to regulatory authorities and relevant external stakeholders, as required or appropriate.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #disaster_recovery | #incident_management | #information_sharing | #risk_management

Response Guidance:

Proactively sharing threat intelligence helps organizations achieve broader cybersecurity situational awareness among internal and external stakeholders.

Describe how the status of recovery activities is promptly communicated to regulatory authorities and relevant external stakeholders, as required or appropriate.

Examples of Effective Evidence:

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-084: Cyber Threat Intelligence Sharing and Distribution Documents

- Policies and procedures for collecting, analyzing, and distributing cyber threat intelligence within the organization and with external partners.
- Agreements or memberships with threat intelligence sharing platforms or industry groups.
- Records of threat intelligence briefings or alerts issued to relevant stakeholders.
- Evaluations of the threat intelligence program, assessing its contribution to the organization's security posture.

EEE-101: Cyber Threat Intelligence Sharing Documentation

- Cyber threat intelligence policies that outline the process for collecting, analyzing, and sharing threat information.
- Records of threat intelligence received and shared with internal stakeholders and external partners.
- Analysis reports based on threat intelligence that inform security strategies and operations.
- Training records for security analysts on threat intelligence tools and analysis techniques.
- Membership or participation records in threat intelligence sharing platforms or industry groups.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

RECOVER / Incident Recovery Communication / Public Information Sharing

RC.CO-04.01: Pre-established communication plans and message templates, and authorized protocols, contacts, media, and communications, are used to notify and inform the public and key external stakeholders about an incident.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #disaster_recovery | #incident_management | #information_sharing | #risk_management

Response Guidance:

Proactive communication and sharing of threat intelligence help organizations achieve broader cybersecurity situational awareness among internal and external stakeholders. The organization's management should ensure that communication plans exist for notifying appropriate parties, including regulators, peer organizations, information sharing organizations and the public.

Describe how the organization's management ensures that a communication plan and message templates, exists to notify the public and key external stakeholders about an incident. Provide information on the stakeholders involved and the process. Provide information on established authorized protocols, contacts, media and communications.

Examples of Effective Evidence:

EEE-030: Board Accountability and Cybersecurity Governance Documentation

- Minutes from board meetings where cybersecurity and risk management topics are discussed, showing oversight and decision-making.
- Policies and procedures that define the roles and responsibilities of senior management in overseeing cybersecurity efforts.
- Performance metrics and reports presented to the board and senior management, demonstrating accountability for security and risk management.
- Documentation of board-approved cybersecurity strategies and initiatives.
- Records of executive training and awareness sessions on cybersecurity and risk management topics.

EEE-071: Customer Cybersecurity Awareness Documentation

- Cybersecurity awareness materials and communications distributed to customers, such as newsletters, alerts, and guidance documents.
- Records of customer-focused cybersecurity events or webinars, including topics covered and attendee feedback.
- Documentation of customer portals or platforms that provide security tips, alerts, and updates.
- Surveys or assessments measuring customer awareness and satisfaction with the organization's cybersecurity communications.
- Case studies or examples of how customer awareness initiatives have successfully mitigated security risks.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EXTEND / Procurement Planning and Due Diligence / Procurement Planning

EX.DD-01.01: Documented procurement plans are developed for initiatives involving elevated business, technical, or cybersecurity risk in order to establish criteria for the evaluation and selection of a supplier, and any special requirements for organizational preparation, supplier due diligence, and contract terms.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #contract_management | #due_diligence | #third_party_risk_management | #vendor_management | #supply_chain_management

Response Guidance:

Procurement plans, evaluation processes of potential suppliers, and contracts with third parties should integrate elevated business, technical, and cybersecurity risk considerations to ensure the organization is managing ongoing supply chain risk. Organizations should establish criteria to assess potential suppliers and perform supplier due diligence.

Describe how the organization plans initiatives involving elevated business, technical, or cybersecurity risk and integrates it into a documented procurement plan. Describe criteria that are established for the evaluation and selection of a supplier. Provide information on how the organization develops special requirements for organizational preparation, supplier due diligence, and contract terms.

Examples of Effective Evidence:

EEE-018: Supplier Evaluation, Onboarding, and Due Diligence Documentation

- Checklists and criteria used for evaluating potential suppliers, including security and resilience factors.
- Due diligence reports for key suppliers, including assessments of their financial stability and operational resilience.
- Agreements that include clauses related to ongoing monitoring and evaluation of supplier performance.
- Records of supplier selection meetings, including rationale for decisions and any identified risks.
- Supplier onboarding process documentation, highlighting security and resilience requirements.

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

EX.DD-01.02: Procurement plans address the inherent risks of the planned activity, to include the complexity of the endeavor in terms of technology, scope, and novelty, and demonstrate that the potential business and financial benefits outweigh the costs to control the anticipated risks.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #contract_management | #third_party_risk_management | #vendor_management | #supply_chain_management

Response Guidance:

Outsourcing to suppliers introduces inherent risks to the organization that should be addressed within the acquisition phase and procurement plan. Risk assessments can be leveraged during project planning and procurement planning to determine whether risks can be mitigated or accepted. Evaluations of inherent risk should include the complexity of the planned activities (e.g., technology, scope, novelty).

Describe how documented procurement plans address the inherent risks of the planned activity. Provide information about how the organization addresses the complexity of the endeavor in terms of technology, scope, novelty, and other factors. Describe how the organization demonstrates that the potential business and financial benefits outweigh the costs to control the anticipated risks. Provide information of documented processes to evaluate potential business and financial benefits.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-018: Supplier Evaluation, Onboarding, and Due Diligence Documentation

- Checklists and criteria used for evaluating potential suppliers, including security and resilience factors.
- Due diligence reports for key suppliers, including assessments of their financial stability and operational resilience.
- Agreements that include clauses related to ongoing monitoring and evaluation of supplier performance.
- Records of supplier selection meetings, including rationale for decisions and any identified risks.
- Supplier onboarding process documentation, highlighting security and resilience requirements.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

EX.DD-01.03: Procurement plans address expected resource requirements and procedures for ongoing management and monitoring of the selected supplier, contingency plans for supplier non-performance, and specific considerations related to contract termination (e.g., return of data).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #contract_management | #third_party_risk_management | #vendor_management | #supply_chain_management

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

The organization should establish formal processes for ongoing management and monitoring third parties. Documented procedures should be established to manage and monitor third-party relationships commensurate with the risk each third party poses to the organization. Organizations should allocate resources with the requisite knowledge and experience to manage ongoing third party risks. Procurement plans should also have a developed contingency plan or exit strategy in the event that a third-party service provider happens to breach a contract or not perform according to the service level agreements.

Describe how procurement plans address expected resource requirements to manage ongoing third party risks. Provide information about established procedures for ongoing management and monitoring of the selected supplier. Provide information about contingency plans established for supplier non-performance. Describe processes and specific considerations related to contract termination.

Examples of Effective Evidence:

EEE-018: Supplier Evaluation, Onboarding, and Due Diligence Documentation

- Checklists and criteria used for evaluating potential suppliers, including security and resilience factors.
- Due diligence reports for key suppliers, including assessments of their financial stability and operational resilience.
- Agreements that include clauses related to ongoing monitoring and evaluation of supplier performance.
- Records of supplier selection meetings, including rationale for decisions and any identified risks.
- Supplier onboarding process documentation, highlighting security and resilience requirements.

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-020: Vendor Contingency and Transition Planning Documents

- Contingency plans for transitioning services in case of vendor failure, including timelines and responsibilities.
- Checklists for evaluating vendor contingency and recovery capabilities during the selection process.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of transition exercises or drills conducted to test the effectiveness of contingency plans.
- Vendor exit strategy documents that outline procedures for terminating relationships while maintaining operational continuity.
- Records of vendor performance issues that triggered contingency or transition plans.

EEE-025: Vendor Contingency and Risk Mitigation Documentation

- Contingency plans that outline alternative solutions in case of vendor failure or service disruption.
- Risk assessments that identify potential points of failure with vendors and corresponding contingency options.
- Documentation of the evaluation and selection process for alternative vendors or solutions.
- Communication plans for engaging with alternative vendors during a contingency event.
- Test results from contingency plan exercises, demonstrating the viability of alternative solutions.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

EXTEND / Procurement Planning and Due Diligence / Prospective Third Party Due Diligence

EX.DD-02.01: The organization implements procedures, and allocates sufficient resources with the requisite knowledge and experience, to conduct third party due diligence and risk assessment consistent with the procurement plan and commensurate with level of risk, criticality, and complexity of each third-party relationship.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #due_diligence | #third_party_risk_management | #vendor_management | #supply_chain_management

Response Guidance:

The organization should establish formal procedures to establish, manage, and monitor its third party relationships commensurate with the risk each third party poses to the organization. Organizations should allocate resources with the requisite knowledge and experience to manage ongoing third

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

party risks. Procedures should establish processes for conducting third party due diligence and risk assessment consistent with the procurement plan.

Describe how the organization allocates sufficient resources with the requisite knowledge and experience to conduct due diligence and manage and monitor its third party relationships. Describe how the organization establishes procedures to conduct third party due diligence and risk assessment consistent with the procurement plan and commensurate with the level of risk, criticality, and complexity of each third party relationship.

Examples of Effective Evidence:

EEE-018: Supplier Evaluation, Onboarding, and Due Diligence Documentation

- Checklists and criteria used for evaluating potential suppliers, including security and resilience factors.
- Due diligence reports for key suppliers, including assessments of their financial stability and operational resilience.
- Agreements that include clauses related to ongoing monitoring and evaluation of supplier performance.
- Records of supplier selection meetings, including rationale for decisions and any identified risks.
- Supplier onboarding process documentation, highlighting security and resilience requirements.

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EX.DD-02.02: The organization reviews and evaluates the proposed business arrangement, to include the proposed fee structures, incentives, and penalties, proposed staff resources, viability of proposed approaches, and business terms, to ensure that products or services are being obtained at competitive and reasonable costs and terms.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #contract_management | #staffing_and_resource_management | #vendor_management

Response Guidance:

Procurement planning should include procedures to review and evaluate the proposed business arrangement to ensure the pricing is fair and reasonable. Balancing the benefit of the products and services delivered and costs impaired on the organization should be a key component of the organization's approach to procurement planning.

Describe how the organization reviews and evaluates the proposed business arrangement to ensure that products or services are being obtained at competitive and reasonable costs and terms. Describe documented processes to review and evaluate the proposed fee structure, incentives, penalties, proposed staff resources, viability of proposed approaches, and business terms. Describe how the organization allocates sufficient resources with the requisite knowledge and experience to review and evaluate the proposed business arrangement.

Examples of Effective Evidence:

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

EX.DD-02.03: The organization reviews and evaluates documentation, such as financial statements, independent audit reports, pooled/shared assessments, control test reports, SEC filings, and past and pending litigation, to the extent required to determine a prospective critical third party's soundness as a business and the quality and sustainability of its internal controls.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #due_diligence | #third_party_risk_management | #vendor_management | #supply_chain_management

Response Guidance:

Organizations should determine a prospective critical third party's soundness by performing due diligence and reviewing and evaluating documentation, such as financial statements, independent audit reports, pooled/shared assessments, control test reports, SEC, filings, and past and pending litigation. High-risk vendors may necessitate a more frequent level of review. The organization's contracts with third parties should stipulate requirements for reviews, frequency of reviews, and required documentation to be provided.

Describe how the organization reviews and evaluates documentation to the extent required to determine a prospective critical third party's soundness as a business and the quality and sustainability of its internal controls.

Examples of Effective Evidence:

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

EX.DD-02.04: The organization reviews and assesses the prospective third party's controls for managing its suppliers and subcontractors (fourth and nth parties), any proposed role fourth and nth parties will play in delivering the products or services, and any specific fourth- and nth-party controls or alternative arrangements the organization may require to protect its interests.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #due_diligence | #review_assessment_and_testing | #third_party_risk_management | #supply_chain_management

Response Guidance:

Critical vendors often have third-party relationships that can present risk to their clients if not properly managed. These vendors should have effective third-party risk management programs and controls in place and appropriate methods for demonstrating due diligence over their third-party relationships. Provide information on the process in place and used to confirm that the organization's third-party service providers conduct due diligence of their own third parties (e.g., subcontractors). Describe how the organization reviews and assesses any proposed role fourth and nth parties will pay in delivering the products and services, and any specific fourth- and nth-party controls or alternative arrangements the organization may require to protect its interests.

Examples of Effective Evidence:

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

EXTEND / Procurement Planning and Due Diligence / Technology & Cybersecurity Risk Assessment

EX.DD-03.01: The organization reviews, evaluates, and risk assesses a prospective critical third party's cybersecurity program, including its ability to identify, assess, monitor, and mitigate its cyber risks; the completeness of its policies and procedures; the strength of its technical and administrative controls; and the coverage of its internal and independent control testing programs.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #due_diligence | #review_assessment_and_testing | #third_party_risk_management | #supply_chain_management

Response Guidance:

The organization's management may rely on third parties to provide critical services; however, management remains responsible for ensuring the confidentiality, integrity, and availability of the organization's systems and information. The organization's third parties should be required to follow minimum cybersecurity requirements that meet the required cybersecurity practices of the organization. Procurement due diligence should review and evaluate the effectiveness of a prospective critical third party's cybersecurity program before establishing a relationship.

Describe how the organization reviews and evaluates a prospective critical third party's cybersecurity program. Provide information on how the organization evaluates a critical third party's ability to identify, assess, monitor, and mitigate its cyber risks. Describe how the organization evaluates a critical third party's completeness of policies and procedures, and strength of their technical and administrative controls. Provide information on how the organization evaluates the coverage of a critical third party's internal and independent control testing programs. Describe the documentation, questionnaire, and other information sources used to evaluate vendor security programs.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-018: Supplier Evaluation, Onboarding, and Due Diligence Documentation

- Checklists and criteria used for evaluating potential suppliers, including security and resilience factors.
- Due diligence reports for key suppliers, including assessments of their financial stability and operational resilience.
- Agreements that include clauses related to ongoing monitoring and evaluation of supplier performance.
- Records of supplier selection meetings, including rationale for decisions and any identified risks.
- Supplier onboarding process documentation, highlighting security and resilience requirements.

EEE-021: Third-Party Cybersecurity and Continuity Assessment Documentation

- Reports from cybersecurity assessments conducted on third-party vendors, including findings and recommendations.
- Third-party business continuity plans that detail recovery strategies and objectives relevant to services provided (or records of plan reviews).
- Agreements with third parties that include requirements for cybersecurity measures and business continuity planning.
- Documentation of joint business continuity exercises with critical vendors, including outcomes and improvements.
- Vendor cybersecurity certification records, verifying adherence to industry standards and best practices.

EEE-026: Third-Party Termination and Decommissioning Documentation

- Termination procedures and checklists that outline the steps for ending a relationship with a third party.
- Documentation of data retrieval or transfer processes upon termination of a third-party contract.
- Records of final account settlements and confirmations of service discontinuation.
- Technical closure reports that confirm the secure decommissioning of third-party services and systems.
- Exit interview records or final performance reviews with the third party, capturing lessons learned and final assessments.

EEE-084: Cyber Threat Intelligence Sharing and Distribution Documents

- Policies and procedures for collecting, analyzing, and distributing cyber threat intelligence within the organization and with external partners.
- Agreements or memberships with threat intelligence sharing platforms or industry groups.
- Records of threat intelligence briefings or alerts issued to relevant stakeholders.
- Evaluations of the threat intelligence program, assessing its contribution to the organization's security posture.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

EEE-101: Cyber Threat Intelligence Sharing Documentation

- Cyber threat intelligence policies that outline the process for collecting, analyzing, and sharing threat information.
- Records of threat intelligence received and shared with internal stakeholders and external partners.
- Analysis reports based on threat intelligence that inform security strategies and operations.
- Training records for security analysts on threat intelligence tools and analysis techniques.
- Membership or participation records in threat intelligence sharing platforms or industry groups.

EX.DD-03.02: The organization reviews, evaluates, and risk assesses a prospective critical third party's business continuity program, to include business impact analyses, risk assessments, continuity plans, disaster recovery plans, technology resilience architecture, and response and recovery plans, test plans, and test results.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #business_impact_analysis | #critical_infrastructure | #disaster_recovery | #due_diligence | #resilience | #review_assessment_and_testing | #third_party_risk_management | #supply_chain_management

Response Guidance:

Business disruptions to the third party could pose a risk to the organization and may affect the organization's ability to service clients. Organizations should ensure that a prospective critical third party has a business continuity program in place.

Describe how the organization reviews and evaluates a prospective critical third party's business continuity program. Provide information on how the organization evaluates a critical third party's business continuity processes, including business impact analyses, risk assessments, and program testing. Provide information on how the organization evaluates a critical third party's business continuity plans, including, disaster recovery plans, technology resilience architecture, and response and recovery plans, test plans, and test results.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-018: Supplier Evaluation, Onboarding, and Due Diligence Documentation

- Checklists and criteria used for evaluating potential suppliers, including security and resilience factors.
- Due diligence reports for key suppliers, including assessments of their financial stability and operational resilience.
- Agreements that include clauses related to ongoing monitoring and evaluation of supplier performance.
- Records of supplier selection meetings, including rationale for decisions and any identified risks.
- Supplier onboarding process documentation, highlighting security and resilience requirements.

EEE-021: Third-Party Cybersecurity and Continuity Assessment Documentation

- Reports from cybersecurity assessments conducted on third-party vendors, including findings and recommendations.
- Third-party business continuity plans that detail recovery strategies and objectives relevant to services provided (or records of plan reviews).
- Agreements with third parties that include requirements for cybersecurity measures and business continuity planning.
- Documentation of joint business continuity exercises with critical vendors, including outcomes and improvements.
- Vendor cybersecurity certification records, verifying adherence to industry standards and best practices.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Training materials for staff involved in managing and overseeing third-party relationships.

EEE-100: Resilience Testing and Business Impact Documentation

- Resilience testing plans and procedures, including objectives and expected outcomes.
- Business Impact Assessment (BIA) reports that evaluate the potential effects of disruptions on business operations.
- Records of resilience testing exercises, including scenarios, execution, and lessons learned.
- Documentation of updates to resilience plans based on testing outcomes and BIA findings.
- Stakeholder feedback on the organization's resilience and the impact of potential business disruptions.

EX.DD-03.03: The organization reviews, evaluates, and risk assesses a prospective critical third party's incident response program, to include monitoring and alerting capabilities, incident reporting procedures and protocols, and capabilities for event analysis, problem resolution, and forensic investigation.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #business_impact_analysis | #critical_infrastructure | #due_diligence | #incident_management | #resilience | #review_assessment_and_testing | #third_party_risk_management | #supply_chain_management

Response Guidance:

Incidents that occur within a third party could pose a risk to the organization and may affect the organization’s ability to service clients. Organizations should ensure that a prospective critical third party has a robust incident response program in place.

Describe how the organization reviews and evaluates a prospective critical third party’s incident response program, to include monitoring and alerting capabilities, incident reporting procedures and protocols, and capabilities for event analysis, problem resolution, and forensic investigation.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-018: Supplier Evaluation, Onboarding, and Due Diligence Documentation

- Checklists and criteria used for evaluating potential suppliers, including security and resilience factors.
- Due diligence reports for key suppliers, including assessments of their financial stability and operational resilience.
- Agreements that include clauses related to ongoing monitoring and evaluation of supplier performance.
- Records of supplier selection meetings, including rationale for decisions and any identified risks.
- Supplier onboarding process documentation, highlighting security and resilience requirements.

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EXTEND / Procurement Planning and Due Diligence / Product & Service Due Diligence

EX.DD-04.01: The organization defines and implements procedures for assessing the compatibility, security, integrity, and authenticity of externally-developed or externally-sourced applications, software, software components, and firmware before deployment and upon any major change.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #application_security | #asset_management | #infrastructure_security | #review_assessment_and_testing | #secure_system_development | #security_baselines

Response Guidance:

The organization's management should establish a formal process and/or procedures for evaluating externally developed or externally-sourced applications before deployment and upon any major change.

Provide information on the processes used within the organization to evaluate (e.g., assessing or testing) the compatibility, security, and integrity. Provide information on the processes used within the organization to evaluate the authenticity of externally-developed or externally-sourced applications, software, software components, and firmware before deployment and upon any major change.

Examples of Effective Evidence:

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EX.DD-04.02: The organization reviews and evaluates any technologies or information systems proposed to support a third party's services or activities, to include compatibility with the organization's technology and cybersecurity architectures, interactions and interfaces with existing systems, security controls, operational management and support requirements, and suitability to the task.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #application_security | #architecture | #asset_management | #infrastructure_security | #review_assessment_and_testing | #secure_system_development | #security_baselines

Response Guidance:

Due diligence conducted on a third party should include evaluations of any technologies or information systems proposed to support a third party's services or activities, to include compatibility with the organization's technology and cybersecurity architectures, interactions and interfaces with existing systems, security controls, operational management and support requirements, and suitability to the task.

Provide information on how the organization reviews and evaluates any technologies or information systems proposed to support a third party's services or activities.

Examples of Effective Evidence:

EEE-018: Supplier Evaluation, Onboarding, and Due Diligence Documentation

- Checklists and criteria used for evaluating potential suppliers, including security and resilience factors.
- Due diligence reports for key suppliers, including assessments of their financial stability and operational resilience.
- Agreements that include clauses related to ongoing monitoring and evaluation of supplier performance.
- Records of supplier selection meetings, including rationale for decisions and any identified risks.
- Supplier onboarding process documentation, highlighting security and resilience requirements.

EEE-112: System Development and Lifecycle Integrity Documentation

- System development lifecycle (SDLC) policies and procedures that ensure integrity throughout the development process.
- Documentation of code reviews, testing results, and quality assurance measures taken during development.
- Version control records and release notes for software development projects.
- Training records for developers on secure coding practices and lifecycle management.
- Audit reports evaluating the adherence to SDLC processes and the integrity of development practices.
- Application Security standard, policies, procedures

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EXTEND / Third-Party Contracts and Agreements / Contract General Requirements

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

EX.CN-01.01: Contracts with suppliers clearly detail the general terms, nature, and scope of the arrangement, to include the distribution of responsibilities between the parties; costs, compensation, reimbursements, incentives, and penalties; service level agreements, performance measures, and benchmarks; responsibilities for providing, receiving, and retaining information; recourse provisions; and the organization's rights to review, monitor, and audit the supplier's activities.

Subject Tags: #contract_management | #information_sharing | #review_assessment_and_testing | #security_logging_monitoring_and_alerting | #staffing_and_resource_management | #third_party_risk_management | #vendor_management | #supply_chain_management

Response Guidance:

The organization should have documented minimum contract requirements for third parties. Describe the organization's process for developing and negotiating contracts with suppliers. Provide information on how the organization creates contracts that clearly details the general terms, nature, and scope of the arrangement. Contracts should include the distribution of roles and responsibilities between parties. Provide information on the contract's documentation of cost, compensation, reimbursement, incentives, and penalties. Describe how the organization outlines service level agreements, performance measures, and benchmarks. Provide information on the contract outlining responsibilities for providing, receiving, and retaining information, as well as recourse provisions, and the organization's rights to review, monitor, and audit the supplier's activities. The organization's management should consider including termination rights and recourse within contracts for a variety of conditions, including failure to meet cybersecurity requirements.

Examples of Effective Evidence:

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-026: Third-Party Termination and Decommissioning Documentation

- Termination procedures and checklists that outline the steps for ending a relationship with a third party.
- Documentation of data retrieval or transfer processes upon termination of a third-party contract.
- Records of final account settlements and confirmations of service discontinuation.
- Technical closure reports that confirm the secure decommissioning of third-party services and systems.
- Exit interview records or final performance reviews with the third party, capturing lessons learned and final assessments.

EX.CN-01.02: Contracts with suppliers address, as relevant to the product or service, the supplier's requirements for managing its own suppliers and partners (fourth parties) and the risks those fourth parties may pose to the third party and to the organization, to include fourth party due diligence, limitations on activities or geography, monitoring, notifications, liability and indemnifications, etc.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #contract_management | #due_diligence | #fourth_party | #information_sharing | #review_assessment_and_testing | #risk_management | #third_party_risk_management | #supply_chain_management

Response Guidance:

Management must require third-party service providers by contract to manage their own suppliers and partners. Suppliers should have risk management processes, plans, and strategies in place to mitigate risks that those fourth parties may post to the third party. Organizations should maintain a third party risk management program that considers risks that fourth parties may impose on the organization.

Describe how the organization's contracts require suppliers to manage their own suppliers and partners (fourth parties) and maintain those practices for the life of the relationship. Describe how the organization ensures that suppliers are performing fourth party due diligence, and considering limitations on activities, or geography. Describe how the organizations ensures that supplies have processes for monitoring, notifications, liability, and indemnifications of a fourth party.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EX.CN-01.03: Contracts with suppliers address, as relevant to the product or service, the implications of foreign-based third or fourth parties, to include the relevance of local laws and regulations, access to facilities and data, limitations on cross-border data transfer, and language and time zone management.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #compliance | #contract_management | #data_protection | #fourth_party | #third_party_risk_management | #vendor_management | #supply_chain_management

Response Guidance:

Contracts with suppliers should be written commensurate with the risk that the supplier poses. Considerations of risks imposed include implications of foreign-based third or fourth parties, to include the relevance of local laws and regulations, access to facilities and data, and limitations on cross-border data transfer, and language and time zone management.

Describe how the organization's contracts address the implications of foreign-based third or fourth parties. Describe processes in place to mitigate the risks of the foreign operations.

Examples of Effective Evidence:

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Change management records for contracts, detailing any amendments related to security and resilience.

EXTEND / Third-Party Contracts and Agreements / Contract Cybersecurity-Related Requirements

EX.CN-02.01: The organization's contracts require third-parties to implement minimum technology and cybersecurity management requirements, to maintain those practices for the life of the relationship, and to provide evidence of compliance on an ongoing basis.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #compliance | #contract_management | #due_diligence | #infrastructure_protection | #third_party_risk_management | #vendor_management | #vulnerability_management | #supply_chain_management

Response Guidance:

Management should require third-party service providers, by contract, to implement appropriate measures designed to meet the organization's minimum cybersecurity requirements and the objectives of regulatory guidelines. Contract clauses should include the organization's right to audit a supplier's activities throughout the relationship, service level agreements, performance measures, timely notification of any security breaches, among others. Organizations should establish an acceptable template contract with consistent clauses that can be used for all third parties.

Describe how the organization's contracts require third parties to implement minimum cybersecurity requirements and to maintain those practices for the life of the relationship. Organizations may need to maintain cybersecurity requirements after the relationship ends (e.g., return of data, escalate the receipt of sensitive data). Describe how contracts address any cybersecurity requirements that extend beyond the relationship with the organization.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-024: Supplier Collaboration and Security Program Documentation

- Joint security initiative plans co-developed with suppliers, outlining collaborative security efforts.
- Meeting minutes from supplier collaboration sessions focused on security topics.
- Shared security roadmaps or project plans that include supplier contributions and responsibilities.
- Documentation of supplier security training programs and participation records.
- Agreements or MOUs that formalize the security collaboration efforts with suppliers.

EEE-105: Stakeholder Obligation Compliance and Sector-Specific Risk Analysis Documents

- Policies and procedures that address stakeholder obligations and sector-specific risks.
- Sector-specific risk analysis reports that identify unique risks and compliance requirements.
- Documentation of compliance audits or assessments, including findings and actions taken to address gaps.
- Agreements or contracts with stakeholders that include compliance with sector-specific obligations and standards.

EX.CN-02.02: Minimum cybersecurity requirements for third-parties include requirements for incident and vulnerability notification, to include the types of events requiring notification, notification timeframes, and escalation protocols.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #contract_management | #due_diligence | #information_sharing | #infrastructure_protection | #third_party_risk_management | #vendor_management | #vulnerability_management | #supply_chain_management

Response Guidance:

The organization's management may rely on third parties to provide critical services; however, management remains responsible for ensuring the confidentiality, integrity, and availability of the organization's systems and information. The organization's third parties should be required to follow minimum cybersecurity requirements that meet the cybersecurity practices of the organization, including requirements for incident and vulnerability notification. These requirements may be documented within service contracts, Requests for Proposals (RFP), and/or other reporting.

Describe the documented minimum cybersecurity requirements for third parties that meet, at a minimum, the cybersecurity practices of the organization. Describe reporting requirements for events requiring notification, escalation protocols and coordination mechanisms. Describe the documented notification timeframes.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EX.CN-02.03: Contracts with suppliers address, as relevant to the product or service, the supplier's obligation to maintain and regularly test a business continuity program and disaster recovery capability the meets the defined resilience requirements of the organization.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #contract_management | #data_backup | #disaster_recovery | #due_diligence | #resilience | #third_party_risk_management | #vendor_management | #supply_chain_management

Response Guidance:

Management should require third-party service providers by contract to maintain and regularly test a business continuity program and disaster recovery capability designed to meet the organization's defined resilience requirements.

Describe how the organization's contracts require suppliers to implement a business continuity program and discovery recovery capability and maintain those practices for the life of the relationship. Describe how contracts address the supplier's obligation to regularly test their business continuity program and discovery recovery capabilityManagement should require third-party service providers by contract to maintain and regularly test a business continuity program and disaster recovery capability designed to meet the organization's defined resilience requirements.

Describe how the organization's contracts require suppliers to implement a business continuity program and discovery recovery capability and maintain those practices for the life of the relationship. Describe how contracts address the supplier's obligation to regularly test their business continuity program and discovery recovery capability.

Examples of Effective Evidence:

EEE-021: Third-Party Cybersecurity and Continuity Assessment Documentation

- Reports from cybersecurity assessments conducted on third-party vendors, including findings and recommendations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Third-party business continuity plans that detail recovery strategies and objectives relevant to services provided (or records of plan reviews).
- Agreements with third parties that include requirements for cybersecurity measures and business continuity planning.
- Documentation of joint business continuity exercises with critical vendors, including outcomes and improvements.
- Vendor cybersecurity certification records, verifying adherence to industry standards and best practices.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EX.CN-02.04: Contracts with suppliers address, as relevant to the product or service, the supplier's obligation to regularly participate in joint and/or bilateral recovery exercises and tests, and to address significant issues identified through recovery testing.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #contract_management | #data_backup | #disaster_recovery | #due_diligence | #resilience | #third_party_risk_management | #vendor_management | #supply_chain_management

Response Guidance:

Management must require third-party service providers by contract to regularly participate in joint and/or bilateral recovery exercises and tests sufficient to support normal operations and obligations following a cybersecurity incident.

Describe how the organization’s contracts require suppliers to regularly participate in joint and/or bilateral recovery exercises and tests and maintain those practices for the life of the relationship. Provide applicable assessment results to demonstrate how the organization and suppliers tested and validated the effectiveness of recovery processes. Describe how contracts address processes for remediating significant issues identified through recovery testing.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-021: Third-Party Cybersecurity and Continuity Assessment Documentation

- Reports from cybersecurity assessments conducted on third-party vendors, including findings and recommendations.
- Third-party business continuity plans that detail recovery strategies and objectives relevant to services provided (or records of plan reviews).
- Agreements with third parties that include requirements for cybersecurity measures and business continuity planning.
- Documentation of joint business continuity exercises with critical vendors, including outcomes and improvements.
- Vendor cybersecurity certification records, verifying adherence to industry standards and best practices.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EXTEND / Monitoring and Managing Suppliers / Ongoing Third-Party Monitoring

EX.MM-01.01: The organization implements procedures, and allocates sufficient resources with the requisite knowledge and experience, to manage and monitor its third-party relationships to a degree and extent commensurate with the risk each third party poses to the organization and the criticality of the third party's products, services, and/or relationship to the organization.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #due_diligence | #policy_management | #staffing_and_resource_management | #third_party_risk_management | #supply_chain_management

Response Guidance:

The organization should conduct ongoing monitoring on all potential third parties before selecting and entering into contracts or relationships with third parties. Organizations should establish a formal third-party risk management program aligned to the organization's risk management program.

Describe how the organization allocates resources with the requisite knowledge and experience to manage ongoing third party risks. Describe how the organization determines the criticality of the third

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

party's products, services, and/or relationship to the organization. Describe documented procedures established to manage and monitor third-party relationships commensurate with the risk each third party poses to the organization.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-020: Vendor Contingency and Transition Planning Documents

- Contingency plans for transitioning services in case of vendor failure, including timelines and responsibilities.
- Checklists for evaluating vendor contingency and recovery capabilities during the selection process.
- Documentation of transition exercises or drills conducted to test the effectiveness of contingency plans.
- Vendor exit strategy documents that outline procedures for terminating relationships while maintaining operational continuity.
- Records of vendor performance issues that triggered contingency or transition plans.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EX.MM-01.02: The organization regularly evaluates its third party relationships to determine if changes in the organization's circumstances, objectives, or third party use warrant a change in a third party's risk rating (e.g., a less critical third-party relationship evolves into being a critical relationship).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #continous_monitoring | #due_diligence | #third_party_risk_management | #supply_chain_management

Response Guidance:

Organizations should have a process to regularly assess and evaluate its third party relationships. Provide information of ongoing third-party monitoring consistent with the organization's third party risk management policies.

Describe how the organization regularly evaluates its third party relationships to determine if there are changes in the organization's circumstances, objectives, or needs. Describe documented processes to update a third party's risk rating if a change is warranted. In particular, the organization should seek to identify situations where a third party starts out as less critical to the organization but becomes critical over time.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EX.MM-01.03: The organization monitors for and regularly evaluates changes in a critical third party's business posture that could pose adverse risk to the organization (e.g., financial condition, reputation, adverse news, compliance/regulatory issues, key personnel, business relationships, consumer complaints, etc.)

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #continous_monitoring | #due_diligence | #third_party_risk_management | #supply_chain_management

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

Organizations should conduct appropriate due diligence on all third parties throughout the life of the relationship. Third-party risk management plans should establish processes for continuous monitoring of third parties to ensure a supplier's business posture is within the organization's risk tolerance. Describe how the organization ensures sufficient risk management if adverse risk to the organization is identified.

Describe how the organization regularly monitors and evaluates changes in a critical third party's business posture. Describe how the organization assesses changes that could pose adverse risk to the organization.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-024: Supplier Collaboration and Security Program Documentation

- Joint security initiative plans co-developed with suppliers, outlining collaborative security efforts.
- Meeting minutes from supplier collaboration sessions focused on security topics.
- Shared security roadmaps or project plans that include supplier contributions and responsibilities.
- Documentation of supplier security training programs and participation records.
- Agreements or MOUs that formalize the security collaboration efforts with suppliers.

EEE-026: Third-Party Termination and Decommissioning Documentation

- Termination procedures and checklists that outline the steps for ending a relationship with a third party.
- Documentation of data retrieval or transfer processes upon termination of a third-party contract.
- Records of final account settlements and confirmations of service discontinuation.
- Technical closure reports that confirm the secure decommissioning of third-party services and systems.
- Exit interview records or final performance reviews with the third party, capturing lessons learned and final assessments.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo
PO Box 1866, Mountain View, CA 94042, USA.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

EEE-105: Stakeholder Obligation Compliance and Sector-Specific Risk Analysis Documents

- Policies and procedures that address stakeholder obligations and sector-specific risks.
- Sector-specific risk analysis reports that identify unique risks and compliance requirements.
- Documentation of compliance audits or assessments, including findings and actions taken to address gaps.
- Agreements or contracts with stakeholders that include compliance with sector-specific obligations and standards.

EX.MM-01.04: The organization regularly assesses critical third party adherence to service level agreements, product specifications, performance metrics, resource level/skill commitments, and quality expectations; addresses performance issues; and exercises contract penalties or credits as warranted.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #continous_monitoring | #contract_management | #critical_infrastructure | #due_diligence | #policy_management | #staffing_and_resource_management | #third_party_risk_management | #supply_chain_management

Response Guidance:

Organizations should formally document processes within the third-party risk management plan to regularly assess critical third party adherence. Contracts should include penalties or credits, as warranted, to be exercised if third parties do not meet expectations to contract requirements.

Describe how the organization regularly assess critical party adherence to contracts. Contracts should include defined service level agreements, product specifications, performance metrics, resource level/skill commitments, and quality expectations. Describe how the organization addresses performance issues. Provide information on how the organization exercises contract penalties or credits, as warranted.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EX.MM-01.05: The organization regularly assesses a critical third party's program and ability to manage its own suppliers and partners (fourth and nth parties) and the risks those fourth and nth parties may pose to the third party and to the organization (e.g., cybersecurity supply chain risk, concentration risk, reputation risk, foreign-party risk, etc.)

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #continous_monitoring | #due_diligence | #fourth_party | #third_party_risk_management | #supply_chain_management

Response Guidance:

As referenced in EX.CN-02.02, the organization has documented minimum cybersecurity requirements for third parties. Third-party risk management plans should have processes to regularly assess a critical third party's program and ability to manage its own suppliers and partners. Organizations should ensure there is visibility with third parties to assess risks of fourth and nth parties. Inherent risks should be assessed within the organization's established risk appetite.

Describe how the organization regularly assess a critical third party's program and ability to manage its own suppliers and partners. Provide information of continuous monitoring performed on suppliers to understand risk exposure.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EX.MM-01.06: The organization regularly reviews the foreign-based operations and activities of a critical third party, or its critical fourth parties, to confirm contract controls are maintained and compliance requirements are managed.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #compliance | #continous_monitoring | #due_diligence | #fourth_party | #third_party_risk_management | #supply_chain_management

Response Guidance:

Contracts should have safeguards to review foreign-based operations and activities of a critical third party, or its critical fourth parties. Formal third-party risk management plans and policies should drive contractual controls to be maintained designed to evaluate risk exposure and manage compliance requirements. Include additional risk management considerations for foreign-based operations and activities.

Describe how the organization regularly reviews foreign-based operations and activities of a critical third party, or its critical fourth parties. Describe how the organization confirms contract controls are maintained and compliance requirements are managed. Describe how the organization regularly assess critical party adherence to contracts. Provide information on how the organization exercises contract penalties or credits, as warranted.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

EEE-105: Stakeholder Obligation Compliance and Sector-Specific Risk Analysis Documents

- Policies and procedures that address stakeholder obligations and sector-specific risks.
- Sector-specific risk analysis reports that identify unique risks and compliance requirements.
- Documentation of compliance audits or assessments, including findings and actions taken to address gaps.
- Agreements or contracts with stakeholders that include compliance with sector-specific obligations and standards.

EXTEND / Monitoring and Managing Suppliers / Ongoing Third-Party Management

EX.MM-02.01: The organization conducts regular third-party reviews for critical vendors to validate that requisite security and contractual controls are in place and continue to be operating as expected.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #compliance | #continous_monitoring | #critical_infrastructure | #due_diligence | #third_party_risk_management | #supply_chain_management

Response Guidance:

The organization may rely on third parties to provide critical services; however, management remains responsible for overseeing the effectiveness of the services provided by third-party service providers. High-risk vendors may necessitate a more frequent and detailed level of review. The organization may employ third party services that monitor the security posture of critical third parties. Third-party reviews may include audits, operational performance reports, financial condition, or other assessments. The organization's contracts with third parties should stipulate requirements for reviews, frequency of reviews, and required documentation. Describe how the organization conducts regular third-party reviews for critical vendors to validate that requisite and contractual controls have been implemented and continue to be operating as expected. Provide information on how the organization tracks results of regular third-party reviews for critical vendors within the organization.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-021: Third-Party Cybersecurity and Continuity Assessment Documentation

- Reports from cybersecurity assessments conducted on third-party vendors, including findings and recommendations.
- Third-party business continuity plans that detail recovery strategies and objectives relevant to services provided (or records of plan reviews).
- Agreements with third parties that include requirements for cybersecurity measures and business continuity planning.
- Documentation of joint business continuity exercises with critical vendors, including outcomes and improvements.
- Vendor cybersecurity certification records, verifying adherence to industry standards and best practices.

EEE-097: Third-Party Risk Management Documentation

- Third-party risk management policies that establish how vendor risks are assessed and managed.
- Oversight procedures and records of vendor performance reviews, including compliance with security requirements.
- Documentation of vendor risk assessments, including due diligence findings and mitigation measures.
- Contracts and agreements with third parties that include clauses related to risk management and security expectations.
- Training materials for staff involved in managing and overseeing third-party relationships.

EX.MM-02.02: A process is in place to confirm that the organization's critical third-party service providers maintain their business continuity programs, conduct regular resiliency testing, and participate in joint and/or bilateral recovery exercises and tests.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Subject Tags: #compliance | #continous_monitoring | #critical_infrastructure | #due_diligence | #resilience | #third_party_risk_management | #supply_chain_management

Response Guidance:

The organization’s third-party oversight should include reviewing third parties’ business continuity programs, resilience plans, and testing. The organization’s management may also actively participate in joint and/or bilateral recovery exercises and tests.

Provide information on the process in place used to confirm that the organization's critical third-party service providers maintain their business continuity programs. Describe the process in place to

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

confirm that regular resiliency testing is conducted by third parties. Responses should include participation from third parties in joint and/or bilateral recovery exercises and tests.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-021: Third-Party Cybersecurity and Continuity Assessment Documentation

- Reports from cybersecurity assessments conducted on third-party vendors, including findings and recommendations.
- Third-party business continuity plans that detail recovery strategies and objectives relevant to services provided (or records of plan reviews).
- Agreements with third parties that include requirements for cybersecurity measures and business continuity planning.
- Documentation of joint business continuity exercises with critical vendors, including outcomes and improvements.
- Vendor cybersecurity certification records, verifying adherence to industry standards and best practices.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EEE-107: Data Recovery and Information Flow Mapping Documentation

- Data recovery strategy documents that outline procedures for restoring lost or corrupted data.
- Information flow maps that illustrate how data moves through the organization, informing recovery planning.
- Test reports from data recovery exercises, demonstrating the ability to restore data in line with recovery strategies.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of changes to data recovery strategies based on new business processes or technologies.
- Training records for IT staff on data recovery procedures and information flow considerations.

EEE-111: Disaster Recovery and Validation Program Documentation

- Disaster Recovery (DR) plans outlining specific recovery steps for Information Technology (IT) systems and data.
- Schedules and results from regular DR testing, ensuring plans are actionable and up-to-date.
- Change management records for DR plans, capturing updates and justifications.
- Records capturing lessons-learned from exercises and the updating of documentation and plans to reflect the improvements.
- Training and certification records for personnel on DR roles and procedures.
- Review reports assessing DR plan alignment with overall business recovery objectives and Business Impact Analyses (BIAs).

EX.MM-02.03: The organization collaborates with suppliers to maintain and improve the secure use of products, services, and external connections.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #endpoint_security | #infrastructure_protection | #security_logging_monitoring_and_alerting | #third_party_risk_management | #supply_chain_management

Response Guidance:

Describe how the organization collaborates with suppliers (e.g., core processing, online and mobile banking, settlement activities, disaster recovery services, cloud service providers) to maintain and improve the security of products, services, and external connections. Hardware and software vendors may periodically update recommended security settings and configurations, especially when updated product versions are released.

Examples include requiring each vendor to use a single remote access solution, ensuring that vendors do not share credentials, multifactor authentication, and enforcing the concept of least access or privilege.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-024: Supplier Collaboration and Security Program Documentation

- Joint security initiative plans co-developed with suppliers, outlining collaborative security efforts.
- Meeting minutes from supplier collaboration sessions focused on security topics.
- Shared security roadmaps or project plans that include supplier contributions and responsibilities.
- Documentation of supplier security training programs and participation records.
- Agreements or MOUs that formalize the security collaboration efforts with suppliers.

EXTEND / Relationship Termination / Termination Planning

EX.TR-01.01: The organization establishes contingencies to address circumstances that might put a vendor out of business or severely impact delivery of services to the organization, sector-critical systems, or the financial sector as a whole.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #continous_monitoring | #critical_infrastructure | #due_diligence | #resilience | #third_party_risk_management | #supply_chain_management

Response Guidance:

The organization should establish contingencies based on the criticality of the vendor. Contingency plans should include processes for identifying potential alternatives for critical vendors. The organization should also be aware of the additional complexity of on-boarding and off-boarding critical systems and include appropriate controls to manage those unique risks.

Describe the organization's contingencies to address circumstances that might put a critical vendor out of business or severely impact delivery of services to the organization, sector-critical systems, or the critical financial sector as a whole.

Examples of Effective Evidence:

EEE-020: Vendor Contingency and Transition Planning Documents

- Contingency plans for transitioning services in case of vendor failure, including timelines and responsibilities.
- Checklists for evaluating vendor contingency and recovery capabilities during the selection process.
- Documentation of transition exercises or drills conducted to test the effectiveness of contingency plans.
- Vendor exit strategy documents that outline procedures for terminating relationships while maintaining operational continuity.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Records of vendor performance issues that triggered contingency or transition plans.

EEE-025: Vendor Contingency and Risk Mitigation Documentation

- Contingency plans that outline alternative solutions in case of vendor failure or service disruption.
- Risk assessments that identify potential points of failure with vendors and corresponding contingency options.
- Documentation of the evaluation and selection process for alternative vendors or solutions.
- Communication plans for engaging with alternative vendors during a contingency event.
- Test results from contingency plan exercises, demonstrating the viability of alternative solutions.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

EEE-111: Disaster Recovery and Validation Program Documentation

- Disaster Recovery (DR) plans outlining specific recovery steps for Information Technology (IT) systems and data.
- Schedules and results from regular DR testing, ensuring plans are actionable and up-to-date.
- Change management records for DR plans, capturing updates and justifications.
- Records capturing lessons-learned from exercises and the updating of documentation and plans to reflect the improvements.
- Training and certification records for personnel on DR roles and procedures.
- Review reports assessing DR plan alignment with overall business recovery objectives and Business Impact Analyses (BIAs).

EX.TR-01.02: The organization periodically identifies and tests alternative solutions in case a critical external partner fails to perform as expected.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #continous_monitoring | #critical_infrastructure | #due_diligence | #resilience | #third_party_risk_management | #vendor_management | #supply_chain_management

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Response Guidance:

A key aspect of external dependency management is determining and implementing the appropriate controls to address the business risk presented by each external partner and potential alternatives in case the external partner fails to perform as expected. Describe how the organization periodically identifies and tests alternative solutions such as using multiple vendors or a combination of internal and external providers, if available (recognizing that may not always be the case) in case a critical external partner fails to perform as expected. Identify monitoring mechanisms to remediate unmet or failed expectations.

Examples of Effective Evidence:

EEE-020: Vendor Contingency and Transition Planning Documents

- Contingency plans for transitioning services in case of vendor failure, including timelines and responsibilities.
- Checklists for evaluating vendor contingency and recovery capabilities during the selection process.
- Documentation of transition exercises or drills conducted to test the effectiveness of contingency plans.
- Vendor exit strategy documents that outline procedures for terminating relationships while maintaining operational continuity.
- Records of vendor performance issues that triggered contingency or transition plans.

EEE-025: Vendor Contingency and Risk Mitigation Documentation

- Contingency plans that outline alternative solutions in case of vendor failure or service disruption.
- Risk assessments that identify potential points of failure with vendors and corresponding contingency options.
- Documentation of the evaluation and selection process for alternative vendors or solutions.
- Communication plans for engaging with alternative vendors during a contingency event.
- Test results from contingency plan exercises, demonstrating the viability of alternative solutions.

EEE-092: Business Continuity Strategy and Exercises Documentation

- Integrated Business Continuity Plans (BCPs) that address various disruption scenarios, informed by Business Impact Analyses (BIAs).
- Documentation of regular BCP reviews, reflecting business changes and new insights.
- Logs from business continuity exercises, including objectives, execution, and actionable feedback.
- Aggregated stakeholder input on the effectiveness and clarity of continuity plans and exercises.
- Audit summaries evaluating the readiness and thoroughness of business continuity measures.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-111: Disaster Recovery and Validation Program Documentation

- Disaster Recovery (DR) plans outlining specific recovery steps for Information Technology (IT) systems and data.
- Schedules and results from regular DR testing, ensuring plans are actionable and up-to-date.
- Change management records for DR plans, capturing updates and justifications.
- Records capturing lessons-learned from exercises and the updating of documentation and plans to reflect the improvements.
- Training and certification records for personnel on DR roles and procedures.
- Review reports assessing DR plan alignment with overall business recovery objectives and Business Impact Analyses (BIAs).

EX.TR-01.03: The organization has a documented third-party termination/exit plan, to include procedures for timely removal of the third-party access, return of data and property, personnel disposition, and transition of services and support.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Subject Tags: #continous_monitoring | #critical_infrastructure | #due_diligence | #resilience | #third_party_risk_management | #vendor_management | #supply_chain_management

Response Guidance:

Management should have an exit strategy in the event a third-party service provider happens to terminate a contract, breach a contract or not perform according to the service level agreements. The strategy should explain what the organization expects to be done both internally and by the vendor, including processes for terminating access once the relationship with the vendor ends.

Provide information on the documented third-party termination/exit strategy that includes procedures for timely removal of the third-party access, return of data and property, personnel disposition, and transition of services and support.

Refer to EX.TR-01.01 for how to address contingencies for vendors if they go out of business.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.
- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-020: Vendor Contingency and Transition Planning Documents

- Contingency plans for transitioning services in case of vendor failure, including timelines and responsibilities.
- Checklists for evaluating vendor contingency and recovery capabilities during the selection process.
- Documentation of transition exercises or drills conducted to test the effectiveness of contingency plans.
- Vendor exit strategy documents that outline procedures for terminating relationships while maintaining operational continuity.
- Records of vendor performance issues that triggered contingency or transition plans.

EEE-025: Vendor Contingency and Risk Mitigation Documentation

- Contingency plans that outline alternative solutions in case of vendor failure or service disruption.
- Risk assessments that identify potential points of failure with vendors and corresponding contingency options.
- Documentation of the evaluation and selection process for alternative vendors or solutions.
- Communication plans for engaging with alternative vendors during a contingency event.
- Test results from contingency plan exercises, demonstrating the viability of alternative solutions.

EEE-026: Third-Party Termination and Decommissioning Documentation

- Termination procedures and checklists that outline the steps for ending a relationship with a third party.
- Documentation of data retrieval or transfer processes upon termination of a third-party contract.
- Records of final account settlements and confirmations of service discontinuation.
- Technical closure reports that confirm the secure decommissioning of third-party services and systems.
- Exit interview records or final performance reviews with the third party, capturing lessons learned and final assessments.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

EXTEND / Relationship Termination / Termination Practices

EX.TR-02.01: Upon termination of a third-party agreement, the organization ensures that all technical and security matters (access, connections, etc.), business matters (service, support, and ongoing relationship), property matters (data, physical, and intellectual), and legal matters are addressed in a timely manner.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Subject Tags: #asset_management | #continous_monitoring | #critical_infrastructure | #data_protection | #due_diligence | #identity_and_access_management | #third_party_risk_management | #vendor_management | #supply_chain_management

Response Guidance:

Organizations should have plans and processes in place for termination of third-party agreements. Provide information of documented exit strategies commensurate with the risk of the third party. Contracts should detail notification requirements and time frames to address unresolved matters.

Describe how the organization ensures that all technical, security, business, property, and legal matters are addressed in a timely manner upon termination of a third-party agreement. Provide information on associated contractual language.

Examples of Effective Evidence:

EEE-017: Third-Party Risk Management and Communication Documents

- Risk assessment reports for each critical third-party vendor, detailing potential risks and mitigation strategies.
- Communication plan templates for coordinating with third parties during incidents.
- Vendor risk management policy that outlines procedures for assessing and managing third-party risks.
- Records of third-party risk management training provided to staff responsible for vendor relations.
- Documentation of third-party performance reviews, focusing on compliance with security and resilience standards.

EEE-019: Vendor Contract Management and Compliance Oversight Documents

- Templates for contracts with vendors that include specific security and resilience requirements.
- Oversight procedures for ensuring vendors comply with contractual obligations related to security and resilience.
- Audit reports of vendor compliance with contract terms, including any corrective actions taken.
- Documentation of contract review meetings, focusing on performance and adherence to security standards.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

- Change management records for contracts, detailing any amendments related to security and resilience.

EEE-026: Third-Party Termination and Decommissioning Documentation

- Termination procedures and checklists that outline the steps for ending a relationship with a third party.
- Documentation of data retrieval or transfer processes upon termination of a third-party contract.
- Records of final account settlements and confirmations of service discontinuation.
- Technical closure reports that confirm the secure decommissioning of third-party services and systems.
- Exit interview records or final performance reviews with the third party, capturing lessons learned and final assessments.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

APPENDIX A – ABBREVIATIONS

BCM	Business Continuity Management
BYOD	Bring Your Own Device
CAT	Cybersecurity Assessment Tool
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technology
CTO	Chief Technology Officer
FFIEC	Federal Financial Institutions Examination Council
FS-ISAC	Financial Services Information Sharing and Analysis Center
GLBA	Gramm-Leach-Bliley Act
IoT	Internet of things
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KCI	Key Control Indicator
KPI	Key Performance Indicator
KRI	Key Risk Indicator
NIST	National Institute of Standards and Technology
OLA	Operation Level Agreement
PCI-DSS	Payment Card Industry Data Security Standard
SDLC	System Development Life Cycle
SDLP	Systemic Data Loss Prevention
SIEM	Security Information and Event Management
SLA	Service Level Agreement
VM	Virtual Machine

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

APPENDIX B – KEY TERMS

Key terms listed below are sourced from known resources available to help management develop and evaluate information security and cyber resilience, including NIST,[6] the FFIEC IT Examination Handbook,[7] the Financial Stability Board (FSB) Cyber Lexicon,[8] and other regulatory sources and international standards. Several terms below are sourced directly from the Profile Glossary,[9] which defines selected terms used in the Profile with the goal to provide a comprehensive cyber lexicon for the financial services sector.

Key Term	Definition	Source
Acceptable Risk	risk that is understood and tolerated by a user, operator, owner, or accreditor	Profile Glossary
Asset	anything that has value to an organization, including but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software, virtual computing platform, and related hardware	NIST
Asset Inventory	comprehensive record of an organization's hardware, software (e.g., physical and virtual servers, operating systems, and business applications), and data repositories (e.g., customer information files or storage area network)	NCUA ACET 2018, Stmt. #47
Audit	independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures	NIST
Audit Trail	a record showing who as accessed an information system and what operations the user has performed during a given period	NIST
Business Unit	an element or segment of the organization representing a specific business function	Profile Glossary
Critical Infrastructure	system and assets, whether physical or virtual, so vital to an organization that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters	Profile Glossary
Cyber Resilience	the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources. Cyber resiliency is emerging as a key element in any	NIST

[7] Refer to the FFIEC IT Examination Handbooks on the FFIEC website.

[8] Refer to the Financial Stability Board Cyber Lexicon on the FSB website.

[9] Refer to and download the Profile on the CRI website.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Key Term	Definition	Source
	effective strategy for mission assurance, business assurance, or operational resilience.	The MITRE Corporation[10]
Cyber Threat	any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service	Profile Glossary
Dashboard	a graphical user interface which often provides views of multiple data points relevant to a single process or objective.	Profile Glossary
External Dependency	refers to an entity's relationships with outside vendors, suppliers, customers, utilities (such as power and telecommunications), and other external organizations and service providers that the covered entity depends on to deliver services, as well as the information flows and interconnections between the entity and those external parties	(FRB-OCC-FDIC issuances 2016)
External Information System	information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization has no direct control over the application of required security controls or the assessment of control effectiveness	NIST
Information Security Risk	the risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems	NIST
Internal Dependency	refers to the business assets (e.g., workforce, data, technology, and facilities) of a covered entity upon which such entity depends to deliver services, as well as the information flows and interconnections among those assets. Documenting these inherent relationships and integrating internal dependencies into risk management plans demonstrate institutional understanding of the extent to which internal dependencies exist and how they are managed.	(FRB-OCC-FDIC issuances 2016)
Least Privilege	the principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.	NIST
Operational Resilience	the ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions	NIST
RACI	an acronym that stands for responsible, accountable, consulted, informed. A RACI chart is a matrix of all the activities or decision-making authorities undertaken in an organization set against all the people or roles	Profile Glossary
Real-Time		NIST

[10] Refer to MITRE's Cyber Resiliency Design Principles on MITRE's website.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Key Term	Definition	Source
	pertaining to the performance of a computation during the actual time that the related physical process transpires so that the results of the computation can be used to guide the physical process	
Recovery Point Objective	the point in time to which data must be recovered	NIST
Recovery Time Objective	the overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business functions	NIST
Residual Risk	the amount of risk that remains after security measures and controls have been put in place	NIST
Risk	the combination of the probability of an event and its consequence	Profile Glossary
Risk Acceptance	explicit or implicit decision to take a particular risk	Profile Glossary
Risk Appetite	a broad-based description of the desired level of risk that an entity will take in the pursuit of its mission	Profile Glossary
Risk Assessment	a process used to identify and evaluate risk and its potential effects	Profile Glossary
Risk Management	process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or mitigating it to an acceptable level	Profile Glossary
Risk Management Framework	a structured approach used to oversee and manage risk for an enterprise	Profile Glossary
Risk Management Plan/Strategy	document that identifies risks and specifies the actions that have been chosen to manage those risks	Profile Glossary
Risk Management Policy	a statement of the overall intentions and direction of an organization related to risk management	Profile Glossary
Risk Management Process	systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring, and reviewing risk	Profile Glossary
Risk Measurement	a process to determine the likelihood of an adverse event or threat occurring and the potential impact	Profile Glossary
Risk Tolerance	reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve	Profile Glossary
Situational Awareness	the ability to identify, process, and comprehend the critical elements of information through a cyber threat intelligence process that provides a level of understanding that is relevant to act upon to mitigate the impact of a potentially harmful event; within a volume of time and	FSB Cyber Lexicon NIST

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

Key Term	Definition	Source
	space, the perception of an enterprise's security posture and its threat environment	
System Development Life Cycle	the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal	NIST
Third-party Service Provider	Any independent party to whom an entity outsources activities that the entity itself is authorized to perform, including a technology service provider	FFIEC IT Examination Handbook
Three Lines of Defense Model	outlines the essential roles and duties for an organization's risk management framework	Institute of Internal Auditors
First Line of Defense (1LoD)	functions that own and manage risks – comprises operational management and employees who own and manage risks and are responsible for implementing corrective actions to address process and control deficiencies	Institute of Internal Auditors
Second Line of Defense (2LoD)	functions that oversee risks – risk management and compliance functions to help build, monitor, and/or challenge the 1LoD to ensure that its risk management activities are working effectively	Institute of Internal Auditors
Third Line of Defense (3LoD)	functions that provide independent assurance – Internal Audit, which provides the governing body and senior management with comprehensive assurance based on the highest level of independence and objectivity within the organization.	Institute of Internal Auditors
Threat	any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals	Profile Glossary
Threat Analysis	process of formally evaluating the degree of the threat to an information system or enterprise and describing the nature of the threat	Profile Glossary
Threat Assessment	process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat	Profile Glossary
Threat Intelligence	information that provides relevant and sufficient understanding for mitigating the impact of a potentially harmful event	Profile Glossary
User Access Authorization	process for ensuring that every user that accesses an information system for processing, storing, or transmitting information is cleared and authorized to view the data	NIST

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

APPENDIX C – DIAGNOSTIC STATEMENTS & IMPACT TIERS

	DIAGNOSTIC STATEMENT	IMPACT TIER
	GOVERN	
GV.OC-01.01	Technology and cybersecurity strategies, architectures, and programs are formally governed to align with and support the organization's mission, objectives, priorities, tactical initiatives, and risk profile.	1 2 3 4
GV.OC-02.01	The organization's obligation to its customers, employees, and stakeholders to maintain safety and soundness, while balancing size and complexity, is reflected in the organization's risk management strategy and framework, its risk appetite and risk tolerance statements, and in a risk-aware culture.	1 2 3 4
GV.OC-02.02	Technology and cybersecurity risk management strategies identify and communicate the organization's role within the financial services sector as a component of critical infrastructure.	1
GV.OC-02.03	Technology and cybersecurity risk management strategies identify and communicate the organization's role as it relates to other critical infrastructures outside of the financial services sector and the interdependence risks.	1
GV.OC-03.01	The organization's technology and cybersecurity strategy, framework, and policies align and are consistent with the organization's legal, statutory, contractual, and regulatory obligations and ensure that compliance responsibilities are unambiguously assigned.	1 2 3 4
GV.OC-03.02	The organization implements and maintains a documented policy or policies that address customer data privacy that is approved by a designated officer or the organization's appropriate governing body (e.g., the Board or one of its committees).	1 2 3 4
GV.OC-04.01	The organization maintains an inventory of key internal assets, business functions, and external dependencies that includes mappings to other assets, business functions, and information flows.	1 2 3
GV.OC-04.02	The organization documents the business processes that are critical for the delivery of services and the functioning of the organization, and the impacts to the business if those processes are degraded or not functioning.	1 2 3 4
GV.OC-04.03	Resilience requirements to support the delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, and normal operations).	1
GV.OC-04.04	The organization prioritizes the resilience design, planning, testing, and monitoring of systems and other key internal and external dependencies according to their criticality to the supported business functions, enterprise mission, and to the financial services sector.	1 2
GV.OC-05.01	The organization identifies, assesses, and documents the key dependencies, interdependencies, and potential points of failure to support the delivery of critical services (e.g., systems, business processes, workforce, third parties, facilities, etc.)	1 2 3 4
GV.OC-05.02	The organization has prioritized its external dependencies according to their criticality to the supported enterprise mission, business functions, and to the financial services sector.	1 2 3
GV.OC-05.03	The organization defines objectives (e.g., Recovery Time Objective, Maximum Tolerable Downtime, Impact Tolerance) for the resumption of critical operations in alignment with business imperatives, stakeholder obligations, and critical infrastructure dependencies.	1 2 3 4
GV.OC-05.04	Recovery point objectives to support data integrity are consistent with the organization's recovery time objectives, information flow dependencies between systems, and business obligations.	1 2 3

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
GV.RM-01.01	Technology and cybersecurity risk management strategies and frameworks are approved by the governing authority (e.g., the Board or one of its committees) and incorporated into the overall business strategy and enterprise risk management framework.	1 2 3 4
GV.RM-01.02	Technology and cybersecurity risk management strategies and frameworks are informed by applicable international, national, and financial services industry standards and guidelines.	1 2 3 4
GV.RM-01.03	The organization has established, and maintains, technology and cybersecurity programs designed to protect the confidentiality, integrity and availability of its information and operational systems, commensurate with the organization's risk appetite and business needs.	1 2 3 4
GV.RM-01.04	Technology and cybersecurity risk management programs incorporate risk identification, measurement, monitoring, and reporting.	1 2 3 4
GV.RM-01.05	The organization's technology, cybersecurity, resilience, and third-party risk management programs, policies, resources, and priorities are aligned and mutually supporting.	1 2 3
GV.RM-02.01	The governing authority (e.g., the Board or one of its committees) endorses and regularly reviews technology and cybersecurity risk appetite and is regularly informed about the status of, and material changes to, the organization's inherent risk profile.	1 2 3 4
GV.RM-02.02	The organization has established statements of technology and cybersecurity risk tolerance consistent with its risk appetite, and has integrated them into technology, cybersecurity, operational, and enterprise risk management practices.	1 2 3
GV.RM-02.03	Determination of the organization's risk appetite and tolerance includes consideration of the organization's stakeholder obligations, role in critical infrastructure, and sector-specific risk analysis.	1 2 3
GV.RM-03.01	Technology and cybersecurity risk management frameworks and programs are integrated into the enterprise risk management framework.	1 2 3 4
GV.RM-03.02	The organization's business continuity and resilience strategy and program align with and support the overall enterprise risk management framework.	1 2
GV.RM-03.03	Technology and cybersecurity risk management and risk assessment processes are consistent with the organization's enterprise risk management policies, procedures, and methods and include criteria for the evaluation and categorization of enterprise-specific risks and threats.	1 2 3
GV.RM-03.04	Technology and cybersecurity risk management considerations are integrated into daily operations, cultural norms, and management discussions and decision-making, and are tailored to address enterprise-specific risks (both internal and external).	1 2
GV.RM-04.01	The governing authority (e.g., the Board or one of its committees) and senior management provide guidance, direction, and credible challenge in the design and implementation of risk management strategies, assessment of identified risks against risk appetite and risk tolerance, and in the selection of risk treatment approaches.	1 2 3 4
GV.RM-05.01	The organization has a process for monitoring its technology, cybersecurity, and third-party risks, including escalating those risks that exceed risk appetite to management and identifying risks with the potential to impact multiple operating units.	1 2 3 4
GV.RM-05.02	The organization establishes minimum requirements for its third-parties that include how the organizations will communicate and coordinate in times of emergency, including: 1) Joint maintenance of contingency plans; 2) Responsibilities for responding to incidents, including forensic investigations; 3) Planning and testing strategies that address severe events in order to identify single points of failure that would cause wide-scale disruption; and	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
	4) Incorporating the potential impact of an incident into their BCM process and ensure resilience capabilities are in place.	
GV.RM-06.01	Technology and cybersecurity risk management and risk assessment processes and methodologies are documented and regularly reviewed and updated to address changes in the risk profile and risk appetite, the evolving threat environment, and new technologies, products, services, and interdependencies.	1 2 3 4
GV.RM-07.01	The organization has mechanisms in place to ensure that strategies, initiatives, opportunities, and emerging technologies (e.g., artificial intelligence, quantum computing, etc.) are evaluated both in terms of risks and uncertainties that are potentially detrimental to the organization, as well as potentially advantageous to the organization (i.e., positive risks).	1 2
GV.RM-08.01	Technology and cybersecurity risk management frameworks are applied to, and are adapted as needed by, the organization's innovations in technology use and adoption of emerging technologies.	1 2 3 4
GV.RM-08.02	Technology and cybersecurity risk management frameworks are applied to all technology projects and procurements to ensure that security requirements (e.g., data confidentiality, access control, event logging, etc.) are addressed consistently from project onset.	1 2 3 4
GV.RM-08.03	The organization defines, maintains, and uses technical security standards, architectures, processes or practices (including automated tools when practical) to ensure the security of its applications and infrastructure.	1 2 3
GV.RM-08.04	The organization integrates the use of technology architecture in its governance processes to support consistent approaches to security and technology design, integration of third party services, consideration and adoption of new technologies, and investment and procurement decisioning.	1 2 3
GV.RM-08.05	The technology architecture and associated management processes should be comprehensive (e.g., consider the full life cycle of infrastructure, applications, emerging technologies, and relevant data) and designed to achieve security and resilience commensurate with business needs.	1 2
GV.RM-08.06	Technology programs and projects are formally governed and stakeholder engagement is managed to facilitate effective communication, awareness, credible challenge, and decision-making.	1 2 3 4
GV.RM-08.07	Technology projects follow an established project management methodology to manage delivery and delivery risks, produce consistent quality, and achieve business objectives and value.	1 2 3 4
GV.RM-09.01	The organization has an enterprise-wide resilience strategy and program, including architecture, cyber resilience, business continuity, disaster recovery, and incident response, which support its mission, stakeholder obligations, critical infrastructure role, and risk appetite.	1 2 3 4
GV.RM-09.02	The resilience program ensures that the organization can continue operating critical business functions and deliver services to stakeholders, to include critical infrastructure partners, during adverse incidents and cyber attacks (e.g., propagation of malware or extended system outages).	1
GV.SC-01.01	The organization maintains a third-party risk management strategy and program to identify and manage the risks associated with third parties throughout their lifecycles in a timely manner, including in support of sector-critical systems and operations, to ensure alignment within risk appetite.	1 2 3 4
GV.SC-01.02	The organization regularly assesses the risk of its ongoing use of third parties in aggregate, considering factors such as critical service dependencies, vendor concentration,	1 2

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
	geographical/geopolitical exposure, fourth-party impacts, and financial sector co-dependencies.	
GV.SC-02.01	The organization clearly defines, and includes in contractual agreements, the division of cybersecurity and technology risk management responsibilities between the organization and its third parties (e.g., a Shared Responsibilities Model).	1 2 3 4
GV.SC-03.01	The organization's third-party risk management strategy and program aligns with and supports its enterprise, technology, cybersecurity, and resilience risk management frameworks and programs.	1 2 3 4
GV.SC-04.01	The organization regularly identifies, inventories, and risk-ranks third-party relationships that are in place, and addresses any identified relationships that were established without formal approval.	1 2 3 4
GV.SC-08.01	The organization's resilience strategy, plans, tests, and exercises incorporate its external dependencies and critical business partners.	1 2 3 4
GV.SC-09.01	Consideration is specifically given to the implications of organizational third-party dependence, requirements, contracts, and interactions in the design, operation, monitoring, and improvement of policies, procedures, and controls to ensure the fulfillment of business requirements within risk appetite.	1 2 3
GV.RR-01.01	The governing authority (e.g., the Board or one of its committees) oversees and holds senior management accountable for implementing the organization's technology and cybersecurity risk management strategies and frameworks.	1 2 3 4
GV.RR-01.02	The governing authority (e.g., the Board or one of its committees) regularly reviews, oversees, and holds senior management accountable for implementing the organization's third-party risk management strategy and program and for managing the organization's ongoing risks associated with the aggregate and specific use of third parties.	1 2 3 4
GV.RR-01.03	The governing authority (e.g., the Board or one of its committees) regularly reviews, oversees, and holds senior management accountable for implementing the organization's resilience strategy and program and for managing the organization's ongoing resilience risks.	1 2 3 4
GV.RR-01.04	The organization has designated a qualified Cybersecurity Officer (e.g., CISO) who is responsible and accountable for developing cybersecurity strategy, overseeing and implementing its cybersecurity program, and enforcing its cybersecurity policy.	1 2 3 4
GV.RR-01.05	The organization designates a qualified Technology Officer (e.g., CIO or CTO) who is responsible and accountable for developing technology strategy, overseeing and implementing its technology program, and enforcing its technology policy.	1 2 3 4
GV.RR-02.01	The roles, responsibilities, qualifications, and skill requirements for personnel (employees and third parties) that implement, manage, and oversee the technology, cybersecurity, and resilience programs are defined, aligned, coordinated, and holistically managed.	1 2 3 4
GV.RR-02.02	The organization has established and assigned roles and responsibilities for systematic cybersecurity threat identification, monitoring, detection, and event reporting processes, and ensures adequate coverage and organizational alignment for these functions.	1 2 3
GV.RR-02.03	Resilience program roles and responsibilities are assigned to management across the organization to ensure risk assessment, planning, testing, and execution coverage for all critical business functions.	1 2 3 4
GV.RR-02.04	Roles and responsibilities for the Third-Party Risk Management Program and for each third-party engagement are defined and assigned.	1 2 3 4
GV.RR-02.05	Personnel (employees and third parties) who fulfill the organization's physical security and cybersecurity objectives understand their roles and responsibilities.	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
GV.RR-02.06	Roles and responsibilities for the inventory, ownership, and custodianship of applications, data and other technology assets are established and maintained.	1 2 3
GV.RR-02.07	Technology and cybersecurity risk management frameworks provide for segregation of duties between policy development, implementation, and oversight.	1 2
GV.RR-03.01	The organization's budgeting and resourcing processes identify, prioritize, and address resource needs to manage identified technology and cybersecurity risks (e.g., skill shortages, headcount, new tools, incident-related expenses, and unsupported systems).	1 2 3 4
GV.RR-03.02	The organization regularly assesses its skill and resource level requirements against its current personnel complement to determine gaps in resource need.	1 2 3 4
GV.RR-03.03	The organization provides adequate resources, appropriate authority, and access to the governing authority for the designated Cybersecurity Officer (e.g., CISO).	1 2 3 4
GV.RR-04.01	The organization conducts (or causes the conduct of) background/screening checks on all personnel (employees and third party) upon hire/retention, at regular intervals throughout employment, and upon a change in role commensurate with their access to critical data and systems.	1 2 3 4
GV.RR-04.02	The organization establishes processes and controls to mitigate cyber risks related to employment termination, as permitted by law, to include the return or disposition of all organizational assets.	1 2 3 4
GV.RR-04.03	The organization integrates insider threat considerations into its human resource, risk management, and control programs to address the potential for malicious or unintentional harm by trusted employees or third parties.	1 2 3
GV.PO-01.01	Technology and cybersecurity policies are documented, maintained and approved by the governing authority (e.g., the Board or one of its committees) or a designated executive.	1 2 3 4
GV.PO-01.02	The accountable governing body, and applicable cybersecurity program and policies, for any given organizational unit, affiliate, or merged entity are clearly established, applied, and communicated.	1 2
GV.PO-01.03	The organization's incentive programs are consistent with cyber risk management objectives, and technology and cybersecurity policies integrate with an employee accountability policy to ensure that all personnel are held accountable for complying with policies.	1 2 3 4
GV.PO-01.04	All personnel (employees and third party) consent to policies addressing acceptable technology use, social media use, personal device use (e.g., BYOD), confidentiality, and/or other security-related policies and agreements as warranted by their position.	1 2 3 4
GV.PO-01.05	Technology and cybersecurity processes, procedures, and controls are established in alignment with cybersecurity policy.	1 2 3 4
GV.PO-01.06	Physical and environmental security policies are implemented and managed.	1 2 3 4
GV.PO-01.07	The organization maintains documented business continuity and resilience program policies and procedures approved by the governing authority (e.g., the Board or one of its committees).	1 2 3 4
GV.PO-01.08	The organization maintains documented third-party risk management program policies and procedures approved by the governing authority (e.g., the Board or one of its committees).	1 2 3 4
GV.PO-02.01	The cybersecurity policy is regularly reviewed, revised, and communicated under the leadership of a designated Cybersecurity Officer (e.g., CISO) to address changes in the risk profile and risk appetite, the evolving threat environment, and new technologies, products, services, and interdependencies.	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
GV.OV-01.01	The governing authority (e.g., the Board or one of its committees) regularly reviews and evaluates the organization's ability to manage its technology, cybersecurity, third-party, and resilience risks.	1 2 3 4
GV.OV-01.02	The designated Cybersecurity Officer (e.g., CISO) periodically reports to the appropriate governing authority (e.g., the Board or one of its committees) or equivalent governing body on the status of cybersecurity within the organization.	1 2 3 4
GV.OV-01.03	The designated Technology Officer (e.g., CIO or CTO) regularly reports to the governing authority (e.g., the Board or one of its committees) on the status of technology use and risks within the organization.	1 2 3 4
GV.OV-02.01	The organization regularly assesses its inherent technology and cybersecurity risks and ensures that changes to the business and threat environment lead to updates to the organization's strategies, programs, risk appetite and risk tolerance.	1 2 3 4
GV.OV-02.02	The organization determines and articulates how it intends to maintain an acceptable level of residual technology and cybersecurity risk as set by the governing authority (e.g., the Board or one of its committees).	1 2 3
GV.OV-03.01	The organization develops, implements, and reports to management and the governing body (e.g., the Board or one of its committees) key technology and cybersecurity risk and performance indicators and metrics to measure, monitor, and report actionable indicators.	1 2 3
GV.OV-03.02	Resilience program performance is measured and regularly reported to senior executives and the governing authority (e.g., the Board or one of its committees).	1 2 3 4
GV.IR-01.01	The organization's enterprise-wide technology and cybersecurity risk management frameworks align with and support an independent risk management function that provides assurance that the frameworks are implemented consistently and as intended.	1 2 3
GV.IR-01.02	The independent risk management function has sufficient independence, stature, authority, resources, and access to the governing body (e.g., the Board or one of its committees), including reporting lines, to ensure consistency with the organization's risk management frameworks.	1 2 3
GV.IR-01.03	The independent risk management function has an understanding of the organization's structure, technology and cybersecurity strategies and programs, and relevant risks and threats.	1 2 3
GV.IR-02.01	The independent risk management function regularly evaluates the appropriateness of the technology and cybersecurity risk management programs for the organization's risk appetite and inherent risk environment	1 2 3
GV.IR-02.02	The independent risk management function regularly assesses the organization's controls and cybersecurity risk exposure, identifies opportunities for improvement based on assessment results, and recommends program improvements	1 2 3
GV.IR-03.01	The independent risk management function reports to the governing authority (e.g., the Board or one of its committees) and to the designated risk management officer within the organization on the implementation of the technology and cybersecurity risk management frameworks throughout the organization and its independent assessment of risk posture.	1 2 3
GV.AU-01.01	The organization has an independent audit function (i.e., internal audit group or external auditor) that follows generally accepted audit practices and approved audit policies and procedures.	1 2 3 4
GV.AU-01.02	The organization has an independent audit plan that provides for the evaluation of technology and cybersecurity risk, including compliance with the approved risk management framework, policies, and processes for technology, cybersecurity, and resilience; and how well the	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
	organization adapts to the evolving risk environment while remaining within its stated risk appetite and tolerance.	
GV.AU-01.03	The independent audit function tests technology management, cybersecurity, incident response, and resilience policies and controls.	1 2 3 4
GV.AU-01.04	The independent audit function evaluates and tests third-party risk management policies and controls, identifies weaknesses and gaps, and recommends improvements to senior management and the governing authority (e.g., the Board or one of its committees).	1 2 3 4
GV.AU-01.05	An independent audit function assesses compliance with applicable laws and regulations.	1 2 3 4
GV.AU-02.01	A formal process is in place for the independent audit function to review and update its procedures and audit plans regularly or in response to changes in relevant standards, the technology environment, or the business environment.	1 2 3 4
GV.AU-02.02	A formal process is in place for the independent audit function to update its procedures and audit plans based on changes to the organization's risk appetite, risk tolerance, threat environment, and evolving risk profile.	1 2 3 4
GV.AU-03.01	The independent audit function reviews technology and cybersecurity practices and identifies weaknesses and gaps.	1 2 3 4
GV.AU-03.02	The independent audit function tracks identified issues and corrective actions from internal audits and independent testing/assessments to ensure timely resolution.	1 2 3 4
GV.AU-03.03	The independent audit function reports to the governing authority (e.g., the Board or one of its committees) within the organization, including when its assessment differs from that of the organization, or when risk tolerance has been exceeded in any part of the organization.	1 2 3 4
	IDENTIFY	
ID.AM-01.01	The organization maintains a current and complete asset inventory of physical devices, hardware, and information systems.	1 2 3 4
ID.AM-02.01	The organization maintains a current and complete inventory of software platforms, business applications, and other software assets (e.g., virtual machines and virtual network devices).	1 2 3 4
ID.AM-03.01	The organization maintains current maps of network resources, mobile resources, external connections, network-connected third parties, and network data flows.	1 2 3 4
ID.AM-04.01	Hardware, software, and data assets maintained by or located at suppliers or other third parties are included in asset management inventories and lifecycle management processes as required for effective management and security.	1 2 3 4
ID.AM-05.01	The organization establishes and maintains risk-based policies and procedures for the classification of hardware, software, and data assets based on sensitivity and criticality.	1 2 3
ID.AM-05.02	The organization's hardware, software, and data assets are prioritized for protection based on their sensitivity, criticality, vulnerability, business value, and dependency role in the delivery of critical services.	1 2 3
ID.AM-07.01	The organization maintains a current inventory of the data being created, stored, or processed by its information assets and data flow diagrams depicting key internal and external data flows.	1 2 3
ID.AM-08.01	The organization establishes and maintains asset lifecycle management policies and procedures to ensure that assets are acquired, tracked, implemented, used, decommissioned, and protected commensurate with their sensitivity, criticality, and business value.	1 2 3

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
ID.AM-08.02	The organization establishes policies, and employs methods to identify, assess, and manage technology solutions that are acquired, managed, or used outside of established, governed technology and cybersecurity processes (i.e., "Shadow IT").	1 2 3
ID.AM-08.03	The organization establishes policies, standards, and procedures for data governance, data management, and data retention consistent with its legal obligations and the value of data as an organizational asset.	1 2 3
ID.AM-08.04	The organization's asset management processes ensure the protection of sensitive data throughout removal, transfers, maintenance, end-of-life, and secure disposal or re-use.	1 2 3 4
ID.AM-08.05	The organization defines and implements standards and procedures, consistent with its data retention policy, for destroying or securely erasing data, media, and storage devices when the data is no longer needed.	1 2 3 4
ID.AM-08.06	Minimum cybersecurity requirements for third-parties cover the entire relationship lifecycle, from the acquisition of data through the return or destruction of data, to include limitations on data use, access, storage, and geographic location.	1 2 3 4
ID.RA-01.01	The organization identifies, assesses, and documents risks and potential vulnerabilities associated with assets, to include workforce, data, technology, facilities, services, and connections.	1 2 3 4
ID.RA-01.02	The organization's business units ensure that information regarding cyber risk is shared with the appropriate level of senior management in a timely manner, so that they can address and respond to emerging cyber risk.	1 2 3 4
ID.RA-01.03	The organization establishes and maintains standards and capabilities for ongoing vulnerability management, including systematic scans, or reviews reasonably designed to identify known cyber vulnerabilities and upgrade opportunities, across the organization's environments and assets.	1 2 3 4
ID.RA-02.01	The organization participates actively (in alignment with its business operations, inherent risk, and complexity) in information-sharing groups and collectives (e.g., cross-industry, cross-government and cross-border groups) to gather, distribute and analyze information about cyber practices, cyber threats, and early warning indicators relating to cyber threats.	1 2 3
ID.RA-02.02	The organization shares authorized information on its cyber resilience framework and the effectiveness of protection technologies bilaterally with trusted external stakeholders to promote the understanding of each party's approach to securing systems.	1 2 3
ID.RA-03.01	The organization, on an ongoing basis, identifies, analyzes, correlates, characterizes, and reports threats that are internal and external to the firm.	1 2 3 4
ID.RA-03.02	The organization solicits and considers threat intelligence received from the organization's stakeholders, service and utility providers, and other industry and security organizations.	1 2 3 4
ID.RA-03.03	The organization includes in its threat analysis those cyber threats which could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred in the past.	1 2 3
ID.RA-03.04	The organization regularly reviews and updates its threat analysis methodology, threat information sources, and supporting tools.	1 2 3 4
ID.RA-04.01	The organization's risk assessment approach includes the analysis and characterization of the likelihood and potential business impact of identified risks being realized.	1 2 3 4
ID.RA-05.01	Threats, vulnerabilities, likelihoods, and impacts are used to determine overall technology, cybersecurity, and resilience risk to the organization.	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
ID.RA-05.02	The organization has established threat modeling capabilities to identify how and why critical assets might be compromised by a threat actor, what level of protection is needed for those critical assets, and what the impact would be if that protection failed.	1 2
ID.RA-05.03	The organization's business units assess, on an ongoing basis, the technology, cybersecurity, and resilience risks associated with the activities of the business unit.	1 2 3
ID.RA-05.04	The organization uses scenario planning, table-top-exercises, or similar event analysis techniques to identify vulnerabilities and determine potential impacts to critical infrastructure, technology, and business processes.	1 2 3
ID.RA-06.01	Technology and cybersecurity risk management programs and risk assessment processes produce actionable recommendations that the organization uses to select, design, prioritize, implement, maintain, evaluate, and modify cybersecurity and technology controls.	1 2 3 4
ID.RA-06.02	The implementation of responses to address identified risks (i.e., risk avoidance, risk mitigation, risk acceptance, or risk transfer (e.g., cyber insurance)) are formulated, assessed, documented, and prioritized based on criticality to the business.	1 2 3 4
ID.RA-06.03	Technology and cybersecurity programs identify and implement controls to manage applicable risks within the risk appetite set by the governing authority (e.g., the Board or one of its committees).	1 2 3 4
ID.RA-06.04	The organization assesses the threats, impacts, and risks that could adversely affect the organization's ability to provide services on an ongoing basis, and develops its resilience requirements and plans to address those risks.	1 2 3 4
ID.RA-06.05	The organization defines and implements standards and procedures to prioritize and remediate issues identified in vulnerability scanning or penetration testing, including emergency or zero-day threats and vulnerabilities.	1 2 3 4
ID.RA-06.06	The organization follows documented procedures, consistent with established risk response processes, for mitigating or accepting the risk of vulnerabilities or weaknesses identified in exercises and testing or when responding to incidents.	1 2 3 4
ID.RA-07.01	The organization defines and implements change management standards and procedures, to include emergency change procedures, that explicitly address risk identified both prior to and during a change, any new risk created post-change, as well as the reviewing and approving authorities (e.g., change advisory boards).	1 2 3 4
ID.RA-07.02	Risk-based criteria are used to categorize each system change, to include emergency changes, to determine the necessary change process standards to apply for change planning, rollback planning, pre-change testing, change access control, post-change verification, and change review and approval.	1 2 3
ID.RA-07.03	Technology projects and system change processes ensure that requisite changes in security posture, data classification and flows, architecture, support documentation, business processes, and business resilience plans are addressed.	1 2 3
ID.RA-07.04	Policy exceptions, risk mitigation plans, and risk acceptances resulting from assessments and evaluations, such as testing, exercises, audits, etc., are formally managed, approved, escalated to defined levels of management, and tracked to closure.	1 2 3
ID.RA-07.05	The organization establishes and maintains an exception management process for identified vulnerabilities that cannot be mitigated within target timeframes.	1 2 3 4
ID.RA-08.01	The organization has established enterprise processes for soliciting, receiving and appropriately channeling vulnerability disclosures from: (1) Public sources (e.g., customers and security researchers); (2) Vulnerability sharing forums (e.g., FS-ISAC); and	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
	(3) Third-parties (e.g., cloud vendors); (4) Internal sources (e.g., development teams).	
ID.RA-08.02	The organization has established enterprise processes to analyze disclosed vulnerabilities with a focus on: (1) Determining its validity; (2) Assessing its scope (e.g., affected assets); (3) Determining it's severity and impact; (4) Identifying affected stakeholders or customers; and (5) Analyzing options to respond.	1 2 3 4
ID.IM-01.01	Technology, cybersecurity, and resilience controls are regularly assessed and/or tested for design and operating effectiveness.	1 2 3 4
ID.IM-01.02	The organization implements a regular process to collect, store, report, benchmark, and assess trends in actionable performance indicators and risk metrics (e.g., threat KRIs, security incident metrics, vulnerability metrics, and operational measures).	1 2 3
ID.IM-01.03	The organization establishes specific objectives, performance criteria, benchmarks, and tolerance limits to identify areas that have improved or are in need of improvement over time.	1 2 3
ID.IM-01.04	Technology and cybersecurity programs include elements designed to assess, manage, and continually improve the quality of program delivery in addressing stakeholder requirements and risk reduction.	1 2 3 4
ID.IM-01.05	The organization's third-party risk management program is regularly assessed, reported on, and improved.	1 2 3 4
ID.IM-02.01	The organization conducts regular, independent penetration testing and red team testing on the organization's network, internet-facing systems, critical applications, and associated controls to identify gaps in cybersecurity defenses.	1 2 3 4
ID.IM-02.02	The thoroughness and results of independent penetration testing are regularly reviewed to help determine the need to rotate testing vendors to obtain fresh independent perspectives.	1 2 3
ID.IM-02.03	The organization tests and validates the effectiveness of the incident detection, reporting, and communication processes and protocols with internal and external stakeholders.	1 2 3 4
ID.IM-02.04	The organization's testing program validates the effectiveness of its resilience strategy and response, disaster recovery, and resumption plans on a regular basis or upon major changes to business or system functions, and includes external stakeholders as required.	1 2 3 4
ID.IM-02.05	The organization establishes testing programs that include a range of scenarios, including severe but plausible scenarios (e.g., disruptive, destructive, corruptive), that could affect the organization's ability to service internal and external stakeholders.	1 2 3 4
ID.IM-02.06	The organization designs and tests its systems and processes, and employs third-party support resources (e.g., Sheltered Harbor), to enable recovery of accurate data (e.g., material financial transactions) sufficient to support defined business recovery time and recovery point objectives.	1 2 3 4
ID.IM-02.07	The organization's governing body (e.g., the Board or one of its committees) and senior management are involved in testing as part of a crisis management team and are informed of te results.	1 2
ID.IM-02.08	The organization tests and exercises, independently and in coordination with other critical secto partners, its ability to support sector-wide resilience in the event of extreme financial stress or th instability of external dependencies, such as connectivity to markets, payment systems, clearing entities, messaging services, etc.	1

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
ID.IM-02.09	Corrective actions for gaps identified during security-related, incident management, response plan, and disaster recovery testing are retested and validated, or have a formal risk acceptance or risk exception.	1 2 3
ID.IM-03.01	A formal process is in place to improve protection controls and processes by integrating recommendations, findings, and lessons learned from exercises, testing, audits, assessments, and incidents.	1 2 3 4
ID.IM-03.02	The organization establishes a systematic and comprehensive program to regularly evaluate an improve its monitoring and detection processes and controls as the threat landscape changes, tools and techniques evolve, and lessons are learned.	1 2 3
ID.IM-04.01	The organization's business continuity, disaster recovery, crisis management, and response plans are in place and managed, aligned with each other, and incorporate considerations of cyber incidents.	1 2 3 4
ID.IM-04.02	The organization's incident response and business continuity plans contain clearly defined roles responsibilities, and levels of decision-making authority, and include all needed areas of participation and expertise across the organization and key third-parties.	1 2 3 4
ID.IM-04.03	Recovery plans include service resumption steps for all operating environments, including traditional, alternate recovery, and highly available (e.g., cloud) infrastructures.	1 2
ID.IM-04.04	The organization has plans to identify, in a timely manner, the status of all transactions and member positions at the time of a disruption, supported by corresponding recovery point objectives.	1 2
ID.IM-04.05	Recovery plans include restoration of resilience following a long term loss of capability (e.g., at a alternate site or a third-party), detailing when the plan should be activated and implementation steps.	1 2
ID.IM-04.06	The organization has established and implemented plans to identify and mitigate the cyber risks poses through interconnectedness to sector partners and external stakeholders.	1
ID.IM-04.07	The organization pre-identifies, pre-qualifies, and retains third party incident management support and forensic service firms, as required, that can be called upon to quickly assist with incident response, investigation, and recovery.	1 2 3 4
ID.IM-04.08	The organization regularly reviews response strategy, incident management plans, recovery plans, and associated tests and exercises and updates them, as necessary, based on: (1) Lessons learned from incidents that have occurred (both internal and external to the organization); (2) Current cyber threat intelligence (both internal and external sources); (3) Recent and wide-scale cyber attack scenarios; (4) Operationally and technically plausible future cyber attacks; (5) Organizational or technical environment changes; and, (6) New technological developments.	1 2 3 4
	PROTECT	
PR.AA-01.01	Identities and credentials are actively managed or automated for authorized devices and users (e.g., removal of default and factory passwords, password strength requirements, automatic revocation of credentials under defined conditions, regular asset owner access review, etc.).	1 2 3 4
PR.AA-01.02	Physical and logical access to systems is permitted only for individuals who have a legitimate business requirement, have been authorized, and who are adequately trained and monitored.	1 2 3 4
PR.AA-02.01	The organization authenticates identity, validates the authorization level of a user before grantin access to its systems, limits the use of an account to a single individual, and attributes activities to the user in logs and transactions.	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
PR.AA-03.01	Based on the risk level of a user access or a specific transaction, the organization defines and implements authentication requirements, which may include multi-factor or out-of-band authentication, and may adopt other real-time risk prevention or mitigation tactics.	1 2 3 4
PR.AA-03.02	Decisions to authorize user access to devices and other assets are made with consideration of: (1) Business need for the access; (2) The type of data being accessed (e.g., customer PII, public data); (3) The risk of the transaction (e.g., internal-to-internal, external-to-internal); (4) The organization's level of trust for the accessing agent (e.g., external application, internal user); and (5) The potential for harm.	1 2 3 4
PR.AA-03.03	The organization reduces fraudulent activity and protects reputational integrity through email verification mechanisms (e.g., DMARC, DKIM), call-back verification, secure file exchange facilities, out-of-band communications, customer outreach and education, and other tactics designed to thwart imposters and fraudsters.	1 2 3 4
PR.AA-04.01	Access credential and authorization mechanisms for internal systems and across security perimeters (e.g., leveraging directory services, directory synchronization, single sign-on, federated access, credential mapping, etc.) are designed to maintain security, integrity, and authenticity.	1 2 3 4
PR.AA-05.01	The organization limits access privileges to the minimum necessary and with consideration of separation of duties (e.g., through role-based access control, asset owner access recertification etc.).	1 2 3 4
PR.AA-05.02	The organization institutes controls over privileged system access by strictly limiting and closely managing staff and services with elevated system entitlements (e.g., multi-factor authentication, dual accounts, privilege and time constraints, etc.)	1 2 3 4
PR.AA-05.03	The organization institutes controls over service account (i.e., accounts used by systems to access other systems) lifecycles to ensure strict security over creation, use, and termination; access credentials (e.g., no embedded passwords in code); frequent reviews of account ownership; visibility for unauthorized use; and hardening against malicious insider use.	1 2 3 4
PR.AA-05.04	Specific roles, responsibilities, and procedures to manage the risk of third-party access to organizational systems and facilities are defined and implemented.	1 2 3 4
PR.AA-06.01	The organization manages, protects, and logs physical access to sensitive areas, devices, consoles, equipment, and network cabling and infrastructure.	1 2 3 4
PR.AA-06.02	The organization manages and protects physical and visual access to sensitive information assets and physical records (e.g., session lockout, clean desk policies, printer/facsimile output trays, file cabinet/room security, document labelling, etc.)	1 2 3 4
PR.AT-01.01	All personnel receive cybersecurity awareness training upon hire and on a regular basis.	1 2 3 4
PR.AT-01.02	Cybersecurity awareness training includes, at a minimum, awareness of and competencies for data protection, personal data handling, compliance obligations, working with third parties, detecting cyber risks, and how to report any unusual activity or incidents.	1 2 3 4
PR.AT-01.03	Cybersecurity awareness training is updated on a regular basis to reflect risks and threats identified by the organization, the organization's security policies and standards, applicable laws and regulations, and changes in individual responsibilities.	1 2 3 4
PR.AT-01.04	As new technology is deployed or undergoes change that also requires changes in practices, al impacted personnel (e.g., end-users, developers, operators, etc.) are trained on the new systen and any accompanying technology and cybersecurity risks.	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
PR.AT-02.01	Mechanisms are in place to ensure that the personnel working with cybersecurity and technolog (e.g., developers, DBAs, network admins, etc.) maintain current knowledge and skills related to changing threats, countermeasures, new tools, best practices, and their job responsibilities.	1 2 3 4
PR.AT-02.02	High-risk groups, such as those with elevated privileges or in sensitive business functions (including privileged users, senior executives, cybersecurity personnel and third-party stakeholders), receive cybersecurity situational awareness training for their roles and responsibilities.	1 2 3 4
PR.AT-02.03	All personnel (employee and third party) are made aware of and are trained for their role and operational steps in response and recovery plans.	1 2 3 4
PR.AT-02.04	The organization maintains and enhances the skills and knowledge of the in-house staff performing incident management and forensic investigation activities.	1 2 3
PR.AT-02.05	All third party staff receive cybersecurity awareness and job training sufficient for them to perfor their duties and maintain organizational security.	1 2 3 4
PR.AT-02.06	The organization has established and maintains a cybersecurity awareness program through which the organization's customers are kept aware of new threats and vulnerabilities, basic cybersecurity hygiene practices, and their role in cybersecurity, as appropriate.	1 2 3 4
PR.AT-02.07	The organization's governing body (e.g., the Board or one of its committees) and senior management receive cybersecurity situational awareness training to include appropriate skills and knowledge to: (1) Evaluate and manage cyber risks; (2) Promote a culture that recognizes that staff at all levels have important responsibilities in ensuring the organization's cyber resilience; and (3) Lead by example.	1 2 3 4
PR.AT-02.08	Where the organization's governing authority (e.g., the Board or one of its committees) does no have adequate cybersecurity expertise, they should have direct access to the senior officer responsible for cybersecurity and independent sources of expertise to discuss cybersecurity related matters.	1 2 3 4
PR.DS-01.01	Data-at-rest is protected commensurate with the criticality and sensitivity of the information and alignment with the data classification and protection policy (e.g., through the use of encryption, authentication, access control, segregation, masking, tokenization, and file integrity monitoring).	1 2 3 4
PR.DS-01.02	The organization implements data loss identification and prevention tools to monitor and protect against confidential data theft or destruction by an employee or an external actor.	1 2 3
PR.DS-01.03	The organization defines and implements controls for the protection and use of removable medi (e.g., access/use restrictions, encryption, malware scanning, data loss prevention, etc.)	1 2 3 4
PR.DS-02.01	Data-in-transit is protected commensurate with the criticality and sensitivity of the information ar in alignment with the data classification and protection policy (e.g., through the use of encryptio authentication, access control, masking, tokenization, and alternate transit paths).	1 2 3 4
PR.DS-10.01	Data-in-use is protected commensurate with the criticality and sensitivity of the information and i alignment with the data classification and protection policy (e.g., through the use of encryption, authentication, access control, masking, tokenization, visual shielding, memory integrity monitoring, etc.)	1 2 3 4
PR.DS-11.01	The organization defines and implements standards and procedures for configuring and performing backups and data replications, including defining backup requirements by data/application/infrastructure criticality, segregating (e.g., air-gapping) and securing backups, verifying backup integrity, and performing backup restoration testing.	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
PR.PS-01.01	The organization establishes and maintains standard system security configuration baselines, informed by industry standards and hardening guidelines, to facilitate the consistent application security settings, configurations, and versions.	1 2 3
PR.PS-01.02	The organization's systems are configured to provide only essential capabilities to implement th principle of least functionality.	1 2 3 4
PR.PS-01.03	The organization employs detection measures and performs regular enforcement checks to ensure that non-compliance with baseline security standards are promptly identified and rectifie	1 2 3
PR.PS-01.04	The organization documents its requirements for accurate and resilient time services (e.g., synchronization to a mandated or appropriate authoritative time source) and adopts best practic guidance in implementing and using these services for logging, event correlation, forensic analysis, authentication, transactional processing, and other purposes.	1 2 3 4
PR.PS-01.05	Acceptable encryption standards, methods, and management practices are established in accordance with defined industry standards.	1 2 3 4
PR.PS-01.06	The organization employs defined encryption methods and management practices commensurate with the criticality of the information being protected and the inherent risk of the technical environment where used.	1 2 3 4
PR.PS-01.07	Cryptographic keys and certificates are tracked, managed, and protected throughout their lifecycles, to include for compromise and revocation.	1 2 3 4
PR.PS-01.08	End-user mobile or personal computing devices accessing the organization's network employ mechanisms to protect network, application, and data integrity, such as "Mobile Device Management (MDM)" and "Mobile Application Management (MAM)" technologies, device fingerprinting, storage containerization and encryption, integrity scanning, automated patch application, remote wipe, and data leakage protections.	1 2 3 4
PR.PS-01.09	Endpoint systems implemented using virtualization technologies employ mechanisms to protect network, application, and data integrity, such as restricting access to local network and peripher devices, multi-factor authentication, locking-down device source network locations, and data leakage protections.	1 2 3 4
PR.PS-02.01	The organization defines and implements controls to identify patches to technology assets, assess patch criticality and risk, test patches, and apply patches within risk/criticality-based targ time frames.	1 2 3 4
PR.PS-02.02	The organization establishes standards and practices for ongoing application management to ensure that applications remain secure and continue to meet organizational needs.	1 2
PR.PS-02.03	Technology obsolescence, unsupported systems, and end-of-life decommissioning/replacemen are addressed in a risk-based manner and actively planned for, funded, managed, and securely executed.	1 2 3
PR.PS-03.01	The organization defines and implements controls for the on-site and remote maintenance and repair of the organization's technology assets (e.g., work must be performed by authorized personnel, use of approved procedures and tools, use of original or vendor-approved spare parts).	1 2 3
PR.PS-04.01	The organization establishes and regularly reviews log management standards and practices, t include the types of events to be detected, log content, security and access considerations, monitoring protocols, integrity checking mechanisms, and retention periods.	1 2 3 4
PR.PS-04.02	The organization defines the scope and coverage of audit/log records to be created and monitored (i.e., internal and external environments, devices, and applications/software to be monitored) and has controls in place to ensure that the intended scope is fully covered and that no logging failures are inhibiting the collection of required logs.	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
PR.PS-04.03	The organization's activity logs and other security event logs are generated, reviewed, securely stored, and retained in accordance with data retention obligations and established standards.	1 2 3 4
PR.PS-05.01	The organization has policies, procedures, and tools in place to detect and block malware from infecting networks and systems, including automatically updating malware signatures and behavior profiles on all endpoints.	1 2 3 4
PR.PS-05.02	The organization implements safeguards against unauthorized mobile code (e.g., JavaScript, ActiveX, VBScript, PowerShell, etc.) on mobile, end point, and server systems.	1 2 3 4
PR.PS-05.03	The organization has policies, procedures, and tools in place to detect, isolate, and block the us of attached malware or malicious links present in email or message services.	1 2 3 4
PR.PS-06.01	The organization implements Secure Systems Development Lifecycle processes for in-house software design, configuration, and development, employing best practices from secure-by-design methodologies (e.g., secure coding, code review, application security testing, etc.) durin all phases of both traditional and agile projects.	1 2 3
PR.PS-06.02	The architecture, design, coding, testing, and operationalization of system solutions address the unique security, resilience, technical, and operational characteristics of the target platform environment(s) (e.g., distributed system, mainframe, cloud, API, mobile, database, etc.)	1 2 3
PR.PS-06.03	Functional, operational, resilience, and security requirements for system development and implementation projects are documented, agreed to by relevant stakeholders, and tracked and managed through development, testing, assurance, acceptance, and delivery.	1 2 3
PR.PS-06.04	Systems development and testing tools, processes, and environments employ security mechanisms to protect and improve the integrity and confidentiality of both the SDLC process and the resulting product (e.g., secured code repositories, segmented environments, automated builds, etc.)	1 2 3
PR.PS-06.05	A software security testing and validation strategy is developed and implemented in the development lifecycle of all software projects, defining testing requirements and plans; performing/automating testing, vulnerability scanning, and migration activities; and supporting code integrity verification (e.g., using digital signatures).	1 2 3
PR.PS-06.06	The system development lifecycle remediates known critical vulnerabilities, and critical vulnerabilities discovered during testing, prior to production deployment.	1 2 3
PR.PS-06.07	DevOps/DevSecOps practices and procedures are aligned with Systems Development Lifecycle security operations, and technology service management processes.	1 2
PR.PS-06.08	The design, configuration, security control, and operation of key applications and system service are documented sufficiently to support ongoing management, operation, change, and assessment.	1 2
PR.PS-06.09	End-user developed solutions, to include models used to support critical business processes an decisions, are formally identified and managed in alignment with their criticality and risk.	1 2
PR.PS-06.10	The organization establishes policies and procedures for the secure design, configuration, modification, and operation of databases, data stores, and data analytics platforms consistent with the criticality of the data being managed.	1 2 3
PR.PS-07.01	The organization's technology operations, process verification, error detection, issue management, root cause analysis, and problem management functions are formally documente monitored, and KPIs are regularly reported to stakeholders.	1 2
PR.PS-07.02	Technology service and support functions address stakeholder expectations (e.g., through state requirements, SLAs, or OLAs) and performance is monitored and regularly reported to stakeholders.	1 2

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
PR.IR-01.01	Networks, systems, and external connections are segmented (e.g., using firewalls, software-defined networks, guest wireless networks, etc.) to implement defense-in-depth and access isolation principles.	1 2 3 4
PR.IR-01.02	Network device configurations (e.g., firewall rules, ports, and protocols) are documented, reviewed and updated regularly and upon change to ensure alignment with network access, segmentation, traversal, and deny-all default requirements.	1 2 3 4
PR.IR-01.03	The integrity and resilience of the organization's communications and control network services are enhanced through controls such as denial of service protections, secure name/address resolution, and/or alternate communications paths.	1 2 3
PR.IR-01.04	The organization controls access to its wireless networks and the information that these network process by implementing appropriate mechanisms (e.g., strong authentication for authentication and transmission, preventing unauthorized devices from connecting to the internal networks, restricting unauthorized traffic, and segregating guest wireless networks).	1 2 3 4
PR.IR-01.05	Remote access is carefully controlled (e.g., restricted to defined systems, access is actively managed (e.g., session timeouts, logging, forced disconnect, etc.), and encrypted connections with multi-factor authentication are used).	1 2 3 4
PR.IR-01.06	The organization's production and non-production environments and data are segregated and managed to prevent unauthorized access or changes to the information assets.	1 2 3
PR.IR-01.07	The organization defines and implements controls for securely configuring and operating Operational Technologies, Industrial Control Systems, and Internet-of-Things (IoT) devices (e.g segregated printer networks, resetting of default passwords, etc.)	1 2 3
PR.IR-01.08	The organization implements policies, procedures, end-user agreements, and technical controls to address the risks of end-user mobile or personal computing devices accessing the organization's network and resources.	1 2 3 4
PR.IR-02.01	The organization designs, documents, implements, tests, and maintains environmental and physical controls to meet defined business resilience requirements (e.g., environmental monitoring, dual power and communication sources, regionally separated backup processing facilities, etc.)	1 2 3 4
PR.IR-03.01	The organization implements mechanisms (e.g., failsafe, load balancing, hot swaps, redundant equipment, alternate services, backup facilities, etc.) to achieve resilience requirements in norm and adverse situations.	1 2
PR.IR-04.01	Baseline measures of network and system utilization and transaction activity are captured to support capacity planning and anomalous activity detection.	1 2
PR.IR-04.02	Technology availability and capacity is planned, monitored, managed, and optimized to meet business resilience objectives and reasonably anticipated infrastructure demands.	1 2 3
	DETECT	
DE.CM-01.01	The organization deploys intrusion detection and intrusion prevention capabilities to detect and prevent a potential network intrusion in its early stages for timely containment and recovery.	1 2 3 4
DE.CM-01.02	The organization implements mechanisms, such as alerting and filtering of sudden high volume and suspicious incoming traffic, to detect and mitigate Denial of Service, "bot", and credential stuffing attacks.	1 2 3
DE.CM-01.03	The organization has policies, procedures, and tools in place to monitor for, detect, and block unauthorized network connections and data transfers.	1 2 3

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
DE.CM-01.04	The organization has policies, procedures, and tools in place to monitor for, detect, and block access from/to devices that are not authorized or do not conform to security policy, e.g., unpatched systems.	1 2 3 4
DE.CM-01.05	The organization implements measures to detect and block access to unauthorized, inappropriate, or malicious websites and services (e.g. social media, messaging, file sharing).	1 2 3 4
DE.CM-01.06	The organization employs deception techniques and technologies (e.g., honeypots) to detect ar prevent a potential intrusion in its early stages to support timely containment and recovery.	1
DE.CM-02.01	The organization's controls include monitoring and detection of anomalous activities and potenti intrusion events across the organization's physical environment and infrastructure, including the detection of environmental threats (fire, water, service outages, etc.) and unauthorized physical access to high-risk system components and locations.	1 2 3 4
DE.CM-03.01	Account access, authentication, and authorization activities are logged and monitored, for both users and devices, to enforce authorized access.	1 2 3 4
DE.CM-03.02	The organization's controls actively monitor personnel (both authorized and unauthorized) for access, authentication, usage, connections, devices, and anomalous behavior to rapidly detect potential cybersecurity events.	1 2 3 4
DE.CM-03.03	The organization logs and reviews the activities of privileged users and accounts, and monitorin for anomalous behaviors is implemented.	1 2 3
DE.CM-06.01	The organization reviews, documents, authorizes, and monitors all third-party connections, data transfer mechanisms, and Application Programming Interfaces (APIs).	1 2 3 4
DE.CM-06.02	The organization implements an explicit approval and logging process and sets up automated alerts to monitor and prevent any unauthorized access to a critical system by a third-party servi provider.	1 2 3
DE.CM-09.01	The organization uses integrity checking mechanisms to verify software, firmware and information integrity and provenance (e.g., checksums, Software Bill of Materials, etc.)	1 2
DE.CM-09.02	The organization uses integrity checking mechanisms to verify hardware integrity.	1 2
DE.CM-09.03	The organization has policies, procedures, and tools in place to monitor for, detect, and block th use of unsupported or unauthorized software, hardware, or configuration changes.	1 2 3 4
DE.AE-02.01	The organization performs timely collection of event data, as well as advanced and automated analysis (including the use of security tools such as antivirus and IDS/IPS) on the detected events to: (1) Assess and understand the nature, scope and method of the attack; (2) Predict and block a similar future attack; and (3) Report timely risk metrics.	1 2 3 4
DE.AE-02.02	The organization establishes, documents, and regularly reviews event alert parameters and thresholds, as well as rule-based triggers to support automated responses, when known attack patterns, signatures or behaviors are detected.	1 2 3 4
DE.AE-03.01	The organization implements systematic and real-time logging, collection, monitoring, detection and alerting measures across multiple layers of the organization's infrastructure, including physical perimeters, network, operating systems, applications, data, and external (cloud and outsourced) environments, sufficient to protect the organization's information assets.	1 2 3 4
DE.AE-03.02	The organization performs real-time central analysis, aggregation, and correlation of anomalous activities, network and system alerts, and relevant event and cyber threat intelligence, including both internal and external (cloud and outsourced) environments, to better detect and prevent multifaceted cyber attacks.	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
DE.AE-04.01	The organization has a documented process to analyze and triage incidents to assess root cause, technical impact, mitigation priority, and business impact on the organization, as well as across the financial sector and other third party stakeholders.	1 2 3 4
DE.AE-06.01	The organization has established processes and protocols to communicate, alert, and regularly report potential cyber attacks and incident information, including its corresponding analysis and cyber threat intelligence, to authorized internal and external stakeholders.	1 2 3 4
DE.AE-07.01	The organization implements measures for monitoring external sources (e.g., social media, the dark web, etc.) to integrate with other intelligence information to better detect and evaluate potential threats and compromises.	1 2
DE.AE-07.02	Relevant event data is packaged for subsequent review and triage and events are categorized f efficient handling, assignment, and escalation.	1 2 3
DE.AE-08.01	Defined criteria and severity levels are in place to facilitate the declaration, escalation, organization, and alignment of response activities to response plans within the organization and across relevant third parties.	1 2 3
	RESPOND	
RS.MA-01.01	The organization's response plans are in place and executed during or after an incident, to include coordination with relevant third parties and engagement of third-party incident support services.	1 2 3 4
RS.MA-02.01	Tools and processes are in place to ensure timely detection, inspection, assessment, and analysis of security event data for reliable activation of incident response processes.	1 2 3 4
RS.MA-03.01	The organization categorizes and prioritizes cybersecurity incident response consistent with response plans and criticality of systems and services to the enterprise.	1 2 3 4
RS.MA-04.01	Response activities are centrally coordinated, response progress and milestones are tracked an documented, and new incident information is assimilated into ongoing tasks, assignments, and escalations.	1 2 3
RS.MA-05.01	The organization's incident response plans define severity levels and associated criteria for initiating response plans and escalating event response to appropriate stakeholders and management levels.	1 2 3 4
RS.AN-03.01	The organization performs a thorough investigation to determine the nature and scope of an event, possible root causes, and the potential damage inflicted.	1 2 3 4
RS.AN-06.01	The organization establishes a risk-based approach and procedures for quarantining systems, conducting investigations, and collecting and preserving evidence per best practices and forens standards.	1 2 3
RS.AN-07.01	Incident-related forensic data is captured, secured, and preserved in a manner supporting integrity, provenance, and evidentiary value.	1 2 3
RS.AN-08.01	Available incident information is assessed to determine the extent of impact to the organization and its stakeholders, the potential near- and long-term financial implications, and whether or no the incident constitutes a material event.	1 2 3 4
RS.CO-02.01	The organization's incident response program includes defined and approved escalation protocols, linked to organizational decision levels and communication strategies, including which types of information will be shared, with whom (e.g., the organization's governing authority and senior management), and how information provided to the organization will be acted upon.	1 2 3 4
RS.CO-02.02	In the event of an incident, the organization notifies impacted stakeholders including, as require government bodies, self-regulatory agencies and/or other supervisory bodies, within required timeframes.	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
RS.CO-02.03	The organization maintains and regularly tests incident response communication procedures, with associated contact lists, call trees, and automatic notifications, to quickly coordinate and communicate with internal and external stakeholders during or following an incident.	1 2 3 4
RS.CO-03.01	The organization ensures that cyber threat intelligence is made available, in a secure manner, t authorized staff with responsibility for the mitigation of cyber risks at the strategic, tactical and operational levels within the organization.	1 2 3
RS.CO-03.02	In the event of an incident, the organization shares authorized information, in a defined manner and through trusted channels, to facilitate the detection, response, resumption and recovery of it own systems and those of other partners and critical sector participants.	1 2 3 4
RS.MI-01.01	The organization has established processes to implement vulnerability mitigation plans, involve third-party partners and outside expertise as needed, and contain incidents in a timely manner.	1 2 3 4
RS.MI-02.01	Targeted investigations and actions are taken to ensure that all vulnerabilities, system components, devices, or remnants used or leveraged in an attack (e.g., malware, compromised accounts, open ports, etc.) are removed or otherwise returned to a secure and reliable state, or that plans to address the vulnerabilities are documented.	1 2 3 4
	RECOVER	
RC.RP-01.01	The organization executes its recovery plans, including incident recovery, disaster recovery, and business continuity plans, during or after an incident to resume operations.	1 2 3 4
RC.RP-02.01	The organization's response plans are used as informed guidance to develop and manage task plans, response actions, priorities, and assignments for responding to incidents, but are adapte as necessary to address incident-specific characteristics.	1 2 3 4
RC.RP-02.02	Recovery plans are executed by first resuming critical services and core business functions, while minimizing any potential concurrent and widespread interruptions to interconnected entitie and critical infrastructure, such as energy and telecommunications.	1 2 3 4
RC.RP-03.01	Restoration steps include the verification of backups, data replications, system images, and oth restoration assets prior to continued use.	1 2 3 4
RC.RP-04.01	Restoration steps include the verification of data integrity, transaction positions, system functionality, and the operation of security controls by appropriate organizational stakeholders and system owners..	1 2 3 4
RC.RP-05.01	The organization maintains documented procedures for sanitizing, testing, authorizing, and returning systems to service following an incident or investigation.	1 2
RC.RP-05.02	Business, technology, cybersecurity, and relevant third-party stakeholders confirm that systems data, and services have been returned to functional and secure states and that a stable operational status has been achieved.	1 2 3 4
RC.RP-06.01	Incident management activities are closed under defined conditions and documentation to support subsequent post-mortem review, process improvement, and any follow-on activities is collected and verified.	1 2 3 4
RC.CO-03.01	The organization timely involves and communicates the recovery activities, procedures, cyber risk management issues to the governing body (e.g., the Board or one of its committees), senior management, incident management support teams, and relevant internal stakeholders.	1 2 3 4
RC.CO-03.02	The organization promptly communicates the status of recovery activities to regulatory authoritie and relevant external stakeholders, as required or appropriate.	1 2 3 4
RC.CO-04.01	Pre-established communication plans and message templates, and authorized protocols, contacts, media, and communications, are used to notify and inform the public and key external stakeholders about an incident.	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
	EXTEND	
EX.DD-01.01	Documented procurement plans are developed for initiatives involving elevated business, technical, or cybersecurity risk in order to establish criteria for the evaluation and selection of a supplier, and any special requirements for organizational preparation, supplier due diligence, an contract terms.	1 2 3
EX.DD-01.02	Procurement plans address the inherent risks of the planned activity, to include the complexity c the endeavor in terms of technology, scope, and novelty, and demonstrate that the potential business and financial benefits outweigh the costs to control the anticipated risks.	1 2
EX.DD-01.03	Procurement plans address expected resource requirements and procedures for ongoing management and monitoring of the selected supplier, contingency plans for supplier non-performance, and specific considerations related to contract termination (e.g., return of data).	1 2
EX.DD-02.01	The organization implements procedures, and allocates sufficient resources with the requisite knowledge and experience, to conduct third party due diligence consistent with the procuremen plan and commensurate with level of risk, criticality, and complexity of each third-party relationship.	1 2 3 4
EX.DD-02.02	The organization reviews and evaluates the proposed business arrangement, to include the proposed fee structures, incentives, and penalties, proposed staff resources, viability of propose approaches, and business terms, to ensure that products or services are being obtained at competitive and reasonable costs and terms.	1 2 3 4
EX.DD-02.03	The organization reviews and evaluates documentation, such as financial statements, independent audit reports, pooled/shared assessments, control test reports, SEC filings, and pa and pending litigation, to the extent required to determine a prospective critical third party's soundness as a business and the quality and sustainability of its internal controls.	1
EX.DD-02.04	The organization reviews and assesses the prospective third party's controls for managing its suppliers and subcontractors (fourth and nth parties), any proposed role fourth and nth parties will play in delivering the products or services, and any specific fourth- and nth-party controls or alternative arrangements the organization may require to protect its interests.	1 2 3 4
EX.DD-03.01	The organization reviews and evaluates a prospective critical third party's cybersecurity progran including its ability to identify, assess, monitor, and mitigate its cyber risks; the completeness of its policies and procedures; the strength of its technical and administrative controls; and the coverage of its internal and independent control testing programs.	1 2 3 4
EX.DD-03.02	The organization reviews and evaluates a prospective critical third party's business continuity program, to include business impact analyses, risk assessments, continuity plans, disaster recovery plans, technology resilience architecture, and response and recovery plans, test plans, and test results.	1 2 3 4
EX.DD-03.03	The organization reviews and evaluates a prospective critical third party's incident response program, to include monitoring and alerting capabilities, incident reporting procedures and protocols, and capabilities for event analysis, problem resolution, and forensic investigation.	1 2 3 4
EX.DD-04.01	The organization defines and implements procedures for assessing the compatibility, security, integrity, and authenticity of externally-developed or externally-sourced applications, software, software components, and firmware before deployment and upon any major change.	1 2
EX.DD-04.02	The organization reviews and evaluates any technologies or information systems proposed to support a third party's services or activities, to include compatibility with the organization's technology and cybersecurity architectures, interactions and interfaces with existing systems, security controls, operational management and support requirements, and suitability to the task	1 2 3 4
EX.CN-01.01	Contracts with suppliers clearly detail the general terms, nature, and scope of the arrangement, to include the distribution of responsibilities between the parties; costs, compensation,	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
	reimbursements, incentives, and penalties; service level agreements, performance measures, and benchmarks; responsibilities for providing, receiving, and retaining information; recourse provisions; and the organization's rights to review, monitor, and audit the supplier's activities.	
EX.CN-01.02	Contracts with suppliers address, as relevant to the product or service, the supplier's requirements for managing its own suppliers and partners (fourth parties) and the risks those fourth parties may pose to the third party and to the organization, to include fourth party due diligence, limitations on activities or geography, monitoring, notifications, liability and indemnifications, etc.	1 2 3 4
EX.CN-01.03	Contracts with suppliers address, as relevant to the product or service, the implications of foreign-based third or fourth parties, to include the relevance of local laws and regulations, access to facilities and data, limitations on cross-border data transfer, and language and time zone management.	1 2 3 4
EX.CN-02.01	The organization's contracts require third-parties to implement minimum technology and cybersecurity management requirements, to maintain those practices for the life of the relationship, and to provide evidence of compliance on an ongoing basis.	1 2 3 4
EX.CN-02.02	Minimum cybersecurity requirements for third-parties include requirements for incident and vulnerability notification, to include the types of events requiring notification, notification timeframes, and escalation protocols.	1 2 3 4
EX.CN-02.03	Contracts with suppliers address, as relevant to the product or service, the supplier's obligation maintain and regularly test a business continuity program and disaster recovery capability the meets the defined resilience requirements of the organization.	1 2 3 4
EX.CN-02.04	Contracts with suppliers address, as relevant to the product or service, the supplier's obligation regularly participate in joint and/or bilateral recovery exercises and tests, and to address significant issues identified through recovery testing.	1 2 3 4
EX.MM-01.01	The organization implements procedures, and allocates sufficient resources with the requisite knowledge and experience, to manage and monitor its third-party relationships to a degree and extent commensurate with the risk each third party poses to the organization and the criticality o the third party's products, services, and/or relationship to the organization.	1 2 3 4
EX.MM-01.02	The organization regularly evaluates its third party relationships to determine if changes in the organization's circumstances, objectives, or third party use warrant a change in a third party's ris rating (e.g., a less critical third-party relationship evolves into being a critical relationship).	1 2
EX.MM-01.03	The organization monitors for and regularly evaluates changes in a critical third party's business posture that could pose adverse risk to the organization (e.g., financial condition, reputation, adverse news, compliance/regulatory issues, key personnel, business relationships, consumer complaints, etc.)	1 2 3 4
EX.MM-01.04	The organization regularly assesses critical third party adherence to service level agreements, product specifications, performance metrics, resource level/skill commitments, and quality expectations; addresses performance issues; and exercises contract penalties or credits as warranted.	1 2 3 4
EX.MM-01.05	The organization regularly assesses a critical third party's program and ability to manage its owi suppliers and partners (fourth and nth parties) and the risks those fourth and nth parties may pose to the third party and to the organization (e.g., cybersecurity supply chain risk, concentrati risk, reputation risk, foreign-party risk, etc.)	1 2 3
EX.MM-01.06	The organization regularly reviews the foreign-based operations and activities of a critical third party, or its critical fourth parties, to confirm contract controls are maintained and compliance requirements are managed.	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.

	DIAGNOSTIC STATEMENT	IMPACT TIER
EX.MM-02.01	The organization conducts regular third-party reviews for critical vendors to validate that requisit security and contractual controls are in place and continue to be operating as expected.	1 2 3 4
EX.MM-02.02	A process is in place to confirm that the organization's critical third-party service providers maintain their business continuity programs, conduct regular resiliency testing, and participate ir joint and/or bilateral recovery exercises and tests.	1 2 3
EX.MM-02.03	The organization collaborates with suppliers to maintain and improve the secure use of product services, and external connections.	1 2 3 4
EX.TR-01.01	The organization establishes contingencies to address circumstances that might put a vendor ou of business or severely impact delivery of services to the organization, sector-critical systems, o the financial sector as a whole.	1 2
EX.TR-01.02	The organization periodically identifies and tests alternative solutions in case a critical external partner fails to perform as expected.	1 2
EX.TR-01.03	The organization has a documented third-party termination/exit plan, to include procedures for timely removal of the third-party access, return of data and property, personnel disposition, and transition of services and support.	1 2
EX.TR-02.01	Upon termination of a third-party agreement, the organization ensures that all technical and security matters (access, connections, etc.), business matters (service, support, and ongoing relationship), property matters (data, physical, and intellectual), and legal matters are addresse in a timely manner.	1 2 3 4

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commo PO Box 1866, Mountain View, CA 94042, USA.