CYBER RISK INSTITUTE

The Profile Guidebook

Guidance for Implementing the CRI Profile v2.0 and Responding to its Diagnostic Statements

Last updated: March 2024

Cyber Risk Institute
Washington, DC

CyberRiskInstitute.org

CYBER RISK INSTITUTE

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 50+ 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, contracting oversight, and member engagement on the largest Profile update to date.

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 review. Their work is of tremendous ongoing benefit to the Profile and the industry overall.

-The CRI Team

CYBER RISK INSTITUTE

TABLE OF CONTENTS

Change Log

Section	Change	Page Number
Table of Contents	• Added "Key Response" to Table of Contents	3
Response Key	• Updated "Key Response" section description • Removed "To Be Assessed" from CRI response options • Added "Not Tested" to CRI response option	8
Govern	• Updated Govern Category from Strategy and Framework (GV.SF) to Organizational Context (GV.OC)	10
Identify | Asset Management	• Added the aligned Tier Box for diagnostic statement ID.AM-08.03	116
Protect | Data Security	• Removed PR.DS-09.01 through PR.DS-09.04 as they were duplicates of ID.AM-08.03 through ID.AM-08.06	200 – 203 (Feb. v2.0 Version)
Detect | Continuous Monitoring	• Updated diagnostic statement aligned Tier Box DE.CM-09.02 to include Tier 2	258
Extend | Due Diligence	• Updated diagnostic statement aligned Tier Box EX.DD-01.01 to include Tier 3	296
Appendix C	• Updated to align with above changes	333

CYBER RISK INSTITUTE

ABOUT THE 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 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

---

[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.

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 and Category. Users can navigate to each of the 318 Diagnostic Statements using the navigation pane and table of contents. Each Diagnostic Statement includes the following:

- **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:** Examples of evidence that organizations may provide to support their response to each Diagnostic Statement. The examples of effective evidence should be referenced and used with three considerations:

  a. The examples of effective evidence included for each Diagnostic Statement are not intended to be exclusive, exhaustive, or all-inclusive, but merely guidance about what could be effective in demonstrating compliance and the factual accuracy of a chosen response. The evidence an organization may provide to support a statement is not necessarily limited to the examples provided in the *Profile Guidebook*.

  b. Any or all examples provided may not necessarily apply to all Profile users. Instead, they are intended to be a starting point to aid Profile users in implementing the Profile. Specific responses and the actual evidence to support a response, whether from the examples of Effective Evidence examples or not, are selected at the discretion of each organization.

  c. 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; to paraphrase Einstein: “as simple as possible, but no simpler”. 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 listing of full Diagnostic Statements and the Impact Tiers associated with each statement, refer to Appendix C.

CYBER RISK INSTITUTE

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

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.
- 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.

CYBER RISK INSTITUTE

GOVERN

Organizational Context (GV.OC)

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
✓	✓	✓	✓

Response Guidance

Describe how the technology and cybersecurity strategies, architectures, and programs establishes priorities for the organization's mission, objectives, and activities 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. Technology and cybersecurity strategies and programs should show alignment to elements of the organization's mission and objectives. Provide information on how the appropriate governing body (e.g., Board or senior management) reviews and approves their technology and cybersecurity strategies designed to align with the organization's mission and objective.

Examples of Effective Evidence

- Organizational mission statement
- Cybersecurity program, strategy and framework
- Technology program, strategy and framework
- Related description of services (e.g., service catalog, including both business and IT services) provided by involved teams
- Target operating model (i.e., desired state of operations considering the organization's role in critical infrastructure)
- Board/senior management presentations, meeting minutes
- Organizational charts
- Roles and responsibilities

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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 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

- Risk appetite and tolerance statements
- Board or committee reports and approvals
- Ongoing risk appetite reporting
- Risk escalation processes
- Risk management tracking processes
- Risk training and awareness documentation

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
✓			

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[6] and the UK's Centre for Protection of National Infrastructure (CPNI)[7]. 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[8].

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)[9] or similar organization to address critical sector impacts.

Examples of Effective Evidence

- Technology and cybersecurity risk management strategy and framework
- Relevant Board and committee meeting agendas and minutes that may identify evidence of internal discussion on cybersecurity risk to other critical infrastructures
- Target operating model (i.e., desired state of operations considering the organization's role in critical infrastructure)
- Business impact analysis based on the organization's role in critical infrastructure
- Industry cross sector engagement evidence (e.g., Analysis & Resilience Center for Systemic Risk (ARC) or Cross Market Operational Resilience Group (CMORG) minutes or other artifacts)

[6] European Council Directive 2008/114/EC.

[7] https://www.cpni.gov.uk/critical-national-infrastructure-0.

[8] Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, Executive Order 13636, *Improving Critical Infrastructure Cybersecurity,* Section 9.

[9] https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector.

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
✓			

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[10] and critical functions set[11] are used to identify relevant sectors. In the United Kingdom the Centre for the Protection of National Infrastructure defines critical national infrastructure.[12]

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 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

- Technology and cyber risk management strategies and framework showing consideration as appropriate to other critical infrastructure sectors and functions
- Relevant Board and committee meeting agendas and minutes that may identify evidence of internal discussion on cybersecurity risk to other critical infrastructures
- Target operating models (i.e., the desired state of operations considering the organization's role in critical infrastructure)
- Industry cross sector engagement evidence such as involvement in multi-sector, public-private intelligence centers (e.g., In the United States, the National Counterintelligence and Security Center)

[10] www.cisa.gov/critical-infrastructure-sectors
[11] www.cisa.gov/national-critical-functions-set
[12] https://www.cpni.gov.uk/critical-national-infrastructure-0

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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

- Cybersecurity policy and standards (including approval and revision history)
- Policy roadmap or process document
- Evidence of legal and regulatory updates (e.g., working group action tracker)
- Laws and regulations assessment process, including how laws and regulations are documented in existing policies
- Board reports
- Relevant Board or committee meeting agendas and minutes
- Annual goals plans
- Responsibility assignment matrix/RACI charts that identify compliance responsibilities
- Organization charts with compliance organization units identified

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
✓	✓	✓	✓

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

- Relevant Board or committee (e.g., Risk Committee) meeting agendas and minutes
- Information Security Program supporting Information
- Data privacy policies
- Periodic review and approval process for policies and procedures
- Data classification matrix
- Organizational chart of privacy office, showing Chief Privacy Officer and reporting lines

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
✓	✓	✓	

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 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

- Asset management policies and standards
- Asset inventory documentation and reporting
- Data flow - documenting applications and interfaces policy/procedure
- Service review process - application instance reviews

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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

- Business process management procedure documentation
- Asset inventory with criticality documentation and reporting
- Dependency management policy, standards, and procedures
- Data and system flow documentation
- Business impact assessments

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
✓			

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

- Service continuity plans
- Resiliency testing plans and schedule
- Inventory management reporting
- Critical services inventory and related dependencies
- Resiliency degradation scenarios

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
✓	✓		

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

- Business impact analysis
- List of critical business functions and corresponding systems
- Methodology for prioritizing assets according to criticality
- Evidence of monitoring and any actions taken for anomalies
- Tools used to monitor systems
- Related reporting and examples

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Inventory of critical internal and external dependencies, business functions, systems, and third parties
- Identification criteria of critical external dependencies and related business functions
- Resiliency management policy, standard, and procedures
- Third-party security policy, standard, and procedures
- Third-party risk management program
- Critical third-party reporting or other related reporting
- Critical operations inventory

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
✓	✓	✓	

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

- Inventory of critical external dependencies and business functions
- Identification criteria of critical external dependencies and related business functions
- Third-party security policy, standard, and procedures
- Third-party risk management program
- Critical third-party reporting or other related reporting
- Contract reporting

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Business continuity/resiliency policies, procedures, and plans
- Recovery time objectives (RTO)
- Recovery point objectives (RPO)
- Impact Tolerance analyses
- Critical operations inventory
- Roles and responsibilities for staff involved in resumption of critical operations
- Recent business impact analysis

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
✓	✓	✓	

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

- Data center recovery procedures
- Backup and restore standards inclusive of RTO and RPO
- Business and system impact assessments identifying critical-operations service level agreements and RTO/RPO objectives
- Service continuity planning standards, processes, and plans
- Business continuity/resiliency plans
- Related testing documentation

Risk Management (GV.RM)

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
✓	✓	✓	✓

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

- Technology and cybersecurity risk management strategies and frameworks, including evidence of approval by the Board (or one of its committees) or other appropriate governing authority
- Enterprise risk management frameworks setting authority framework
- Policies, standards, procedures, and guidelines specific to technology and cyber risk management
- Organizational chart to demonstrate functional roles, responsibilities, and independence
- Relevant Board and committee (e.g., cyber risk strategy committee, technology steering committee, etc.) meeting minutes and approvals where technology and cyber risk management strategy is discussed

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
✓	✓	✓	✓

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

- Technology and cyber risk management strategies and frameworks, including evidence of consistency with applicable industry standards and guidelines
- Evidence of a process in place to modify the strategy and/or framework due to changes in international, national, and financial services industry standards and guidelines (e.g., SWIFT, PCI-DSS)
- Relevant Board or committee (e.g., IT Committee, Steering Committee, Governance Committee) meeting agendas and minutes
- Control Library mapping the organization's control environment to known standards and guidelines
- If applicable, evidence of participation in various industry and/or government bodies, including the Financial Services Information Sharing and Analysis Center (FS-ISAC), National ISACs, etc.

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
✓	✓	✓	✓

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

- Technology and Cybersecurity/Information Security Programs
- Program steering committee agenda and minutes
- Relevant Board or committee (e.g., Risk Committee) meeting agendas and minutes
- Technology and cybersecurity action plans (layered security approach)
- Technology and cybersecurity key performance indicators and key risk indicators

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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

Examples of Effective Evidence

- Technology and cyber risk management strategies and frameworks and methodologies
- Description of risk assessment and risk management processes
- Control libraries
- Relevant Board and committee meeting agendas and minutes
- Technology and cyber risk reports and briefings
- Risk control monitoring and self-assessment material (e.g., process maps, GRC reports, etc.)
- Technology and cybersecurity dashboards and/or metrics (monthly, quarterly, annually)
- Reports demonstrating threat intelligence capability to identify new and shifting risks/adversaries/vulnerabilities
- Organization-specific tools or processes to reduce identified risks

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
✓	✓	✓	

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

- Technology, cybersecurity, resilience, and third-party program and policy documentation
- Periodic review and adjustment to resource allocation to align to the strategy and priorities
- Periodic review and update of policies and procedures to align organizational functions

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
✓	✓	✓	✓

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.

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

- Risk appetite statements
- Board reports and approvals
- Committee agendas, minutes, and related terms of reference.
- Ongoing risk appetite reporting
- Risk escalation processes

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
✓	✓	✓	

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

- Relevant Board and committee meeting agendas and minutes
- Cyber risk assessment methodology
- Risk appetite statement, including tolerance levels
- KRIs with clearly defined inner and outer boundaries
- Supporting reports and briefs

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
✓	✓	✓	

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

- Risk appetite documentation (e.g., risk appetite statement, KRIs, metrics, change process, etc.)
- Risk assessment documentation
- Target operating model (i.e., desired state of operations considering the organization's role in critical infrastructure)
- Enterprise risk framework

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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 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

- Technology and cyber risk management strategies and frameworks
- Enterprise risk management strategy and framework
- Technology and cyber risk assessment methodologies
- Target operating model (i.e., desired state of operations considering the organization's role in critical infrastructure)
- Organizational structure
- Governance structure (e.g., three lines of defense)

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
✓	✓		

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

- Cyber risk management strategy and framework
- Security incident response policy, standard, and procedures
- Business continuity/resilience policy, standard, and procedures
- Incident response examples or playbooks
- Risk management framework
- Related reporting

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
✓	✓	✓	

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

- Policies, standards, procedures, and guidelines for implemented risk assessments and risk management (e.g., third-party risk assessments)
- Technology and cybersecurity risk assessment and risk management strategies and methodologies
- Risk assessment tools
- Security control testing standard (consistent with the informative references for this Diagnostic Statement)
- Supporting evidence of tools and processes being applied

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
✓	✓		

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

- Relevant Board and committee meeting agendas and minutes
- Technology and cyber risk reports and briefings
- Risk framework in use (e.g., daily operational reports and briefs, example of reducing high risk at the operational level directly linked to the cyber risk management program)
- Control library mapping control environment to known standards and guidelines
- Overall summary of the three lines of defense

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
✓	✓	✓	✓

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

- Enterprise, Technology, and cybersecurity risk management strategies and frameworks, including evidence of approval by appropriate governing authority
- Relevant Board and committee (e.g., Board Risk, IT Steering, and other oversight committees) charters and meeting minutes, including those where senior management with accountability for enterprise, technology, and cybersecurity strategies are required to present on effectiveness/implementation
- Policies, standards, controls, procedures, and guidelines specific to risk management procedures
- Risk management reporting framework, inclusive of periodic reviews and updates provided to the governing authority
- Documentation and evidence of review of credible challenge

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
✓	✓	✓	✓

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 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

- Risk appetite reports
- Risk tolerance reports
- Security incident response standard
- Guidance for escalating risks if business users believe risks exceed risk appetite
- Process for how business users are made aware of security risks (e.g., training materials, escalation procedures, near misses discovered by front line teams, etc.)
- Risk reporting, dashboards, metrics, indicators (i.e., KRIs, KPIs, etc.) and briefs
- Relevant Board and committee (e.g., Risk committee) meeting agendas and minutes

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:

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

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.**

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract guidance
- Contract clauses
- Contract reporting
- Contingency plans
- Escalation matrix
- Testing strategies
- Related third-party reporting
- Shared security responsibility model (SSRM)

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
✓	✓	✓	✓

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

- Policies, standards, procedures, and guidelines specific to cyber risk management, including evidence of risk assessment process
- Description of the cyber risk assessment process and methodology and how updates are reviewed and approved by various risk functions
- Control environment reporting
- Relevant Board and committee (e.g., Board Risk Committee) meeting agendas and minutes
- Cyber risk assessment reports and briefings

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
✓	✓		

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

- Risk management policy and standards documentation
- Risk management strategy and framework
- Related risk reporting
- Evaluation of inherent risks and positive risks in the enterprise, technology, and cybersecurity strategies, initiatives, and emerging technologies
- Meeting minutes of board and senior management discussions of strategy, initiatives, and new technology adoption

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
✓	✓	✓	✓

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

- Security policy and standards documentation
- Third-party security standards, processes, and reports
- Application/system security standards, processes, and reports
- Secure system development standards and processes, including how cybersecurity risk is incorporated during the beginning of processes
- Security testing standards, processes, and reports
- Other related policies, standards, and 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
✓	✓	✓	✓

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

- Security policy and standards documentation
- Third-party security standards, processes, and reports
- Application/system security standards, processes, and reports
- Secure system development standards and processes, including how cybersecurity risk is incorporated during the beginning of processes
- Security testing standards, processes, and reports
- Opinion papers, assurance reviews, etc. from the independent risk function
- Cyber risk management strategy and framework
- Organization's project management documents (including reference to cyber risk management)
- Project management standards
- Change management standards

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
✓	✓	✓	

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

- Security policy and standards documentation
- Third-party security standards, processes, and reports
- Application, security, and/or infrastructure security standards, processes, and reports
- Secure system development standards and processes
- Security testing standards, processes, and reports
- Other related policies, standards, and procedures (including documentation of security policy reviews)
- Evidence of technical industry frameworks standards used throughout system development lifecycle (e.g., SABSA, NIST 800-53, ISO 27001, etc.)
- Risk management and risk assessment standards

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
✓	✓	✓	

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

- Risk management and governance strategy and framework
- Risk management policy, standard, and procedures
- Documentation of representing the governance within system development, architecture design, and business investment decisions, and considerations of new technologies (i.e., infrastructure, and hardware and software assets, etc.)
- Organization enterprise and technology architectures
- Architecture management standards and procedures
- Meeting minutes and presentations about the organization's enterprise and technology architectures
- Project and procurement documentation referencing the organization's enterprise and technology architectures

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
✓	✓		

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

- Risk management and governance strategy and framework
- Risk management policy, standard, and procedures
- Information security and resilience policy, standard, and procedures
- Software development lifecycle policy, standard, and procedures
- Organization enterprise and technology architectures
- Architecture management standards and procedures
- Meeting minutes and presentations about the organization's enterprise and technology architectures
- Project and procurement documentation referencing the organization's enterprise and technology architectures

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
✓	✓	✓	✓

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

- Organizational reporting structure
- Meeting minutes or additional information as example of credible challenge to business programs and projects, discussions of stakeholder requirements
- Procedures to track and measure project performance against requirements
- Example of project requirements with collaboration among stakeholders
- Project management policy, standard, procedures, and documentation

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
✓	✓	✓	✓

Response Guidance

The organization should follow a standardized project management methodology from project initialization 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 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

- Project management policy, standard, procedures
- Procedures to track and measure project performance against requirements
- Example of project requirements with collaboration among stakeholders
- Organization's project management documents
- Example of project tracking and system of record

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
✓	✓	✓	✓

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

- Cyber risk management strategy and framework
- Security incident response policy, standard, and procedures
- Business continuity/resilience policy, standard, and procedures
- Incident response examples or playbooks
- Related reporting
- Disaster recovery plans
- Operational resilience plans
- Disaster recovery and incident response plan testing

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
✓			

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

- Security incident response policy, standard, and procedures
- Business continuity/resilience policy, standard, and procedures
- Anti-malware security standard
- Anti-virus and anti-malware control
- Incident response examples or playbooks
- Backup and restore policy, standard, and process

Supply Chain Risk Management (GV.SC)

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
✓	✓	✓	✓

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

- Dependency management policy, standards, and procedures
- Third-party security policy, standard, and procedures
- Third-party risk management program
- Inventory of third parties and/or identified critical vendors
- Third party initial risk questionnaire
- Contractual language on security requirements (security schedule)
- Business impact analysis

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
✓	✓		

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 considerations of critical service dependencies, vendor concentration, geographical/geopolitical exposure, fourth-party impacts, and financial sector co-dependencies.

Examples of Effective Evidence

- Dependency management policy, standards, and procedures
- Third-party security policy, standard, and procedures
- Third-party risk management program
- Inventory of third parties and/or identified critical vendors
- Aggregate review of reliance on third-party services and risk associated risks
- Business impact analysis
- Meeting minutes and presentations regarding aggregate or non-specific third party risk

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).

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Vendor management security policy, standard, and procedures
- Vendor management program
- Contract guidance
- Contract clauses
- SSRM documentation

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
✓	✓	✓	✓

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

- Enterprise risk management framework and program documentation
- Operational risk management framework and program documentation
- Cyber risk management framework and program documentation
- Resiliency risk management framework and program documentation
- Technology risk management framework and program documentation
- Third-party security policy, standard, and process
- Third-party risk management program
- Examples of contracts with third parties

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
✓	✓	✓	✓

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Inventory of third-parties and/or identified critical vendors
- Business Impact Analysis
- Third-party risk assessment
- Related reporting and examples

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
✓	✓	✓	✓

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

- Security incident response policy, standard, and procedures
- Business continuity/resilience policy, standard, and procedures
- Incident response examples or playbooks
- Third-party testing plan and after-action reports
- Third-party security policy, standard, and procedures
- Third-party risk management program
- Critical third-party identification processes
- Critical third-party inventory

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
✓	✓	✓	

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

Examples of Effective Evidence

- Third-party security policy, standard, and procedures
- Third-party risk management program documentation
- Vendor management policy, standard, and procedures
- Risk appetite statements
- Other related third-party assessment processes, examples, and reporting

Roles, Responsibilities, and Authorities (GV.RR)

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
✓	✓	✓	✓

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 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

- Technology and cybersecurity risk management strategies and frameworks, including evidence of approval by appropriate governing authority
- Policies, standards, controls, procedures, and guidelines specific to technology and cybersecurity risk management
- Relevant Board and committee (e.g., Board Risk, IT Steering, and other oversight committees) charters and meeting minutes, including those where senior management with accountability for cybersecurity strategy are required to present on effectiveness/implementation
- Gramm-Leach-Bliley Act (GLBA) compliance report
- Organizational charts to demonstrate accountable individuals, roles, and responsibilities for technology and cybersecurity risk management
- Senior management scorecards on operating effectiveness, including KPIs and KRIs

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
✓	✓	✓	✓

Response Guidance

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Third party management governance roles and responsibilities
- Due diligence policy, requirement, or questionnaire
- Other related third-party assessment processes, examples, and reporting
- Meeting minutes and presentations on key procurements and aggregate third-party use and risks

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
✓	✓	✓	✓

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

- Resilience strategy and program, including evidence of approval by appropriate governing authority
- Policies, standards, controls, procedures, and guidelines specific to resilience
- Relevant Board and committee charters and meeting minutes, including those where senior management with accountability for cyber strategy are required to present on effectiveness/implementation

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
✓	✓	✓	✓

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

- Organizational structure, including designated persons, teams, organizations, and departments
- Job Description/CV of CISO (or designated Cybersecurity Officer)
- Engagement of consultants and professional services, as applicable
- Board approvals
- Related description of services provided by involved teams (e.g., service catalog)
- Description of overall budget process, including cybersecurity

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
✓	✓	✓	✓

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

- Organizational structure, including designated persons, teams, organizations, and departments
- Job Description/CV of CIO or CTO (or designated Technology Officer)
- Description of overall budget process, including technology
- Board approvals
- Related description of services provided by involved teams

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Organizational structure
- IT security roles and responsibilities documents
- Related training, certification, and skillset requirements
- Related description of services provided by involved teams
- Sample cybersecurity job descriptions/profiles
- Workforce assessments (e.g., performance assessments)
- Cybersecurity job profiles
- Cyber resilience resourcing including threat analysis, security operations, and incident response
- Risk appetite statements and risk metrics
- Relevant Board or committee meeting agendas and minutes where roles and responsibilities or effectiveness are discussed
- Third party contracts
- Third party SSRM
- Resource gap assessments

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
✓	✓	✓	

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

- Organizational structure documents including defined responsibilities for the incident response team
- Related job descriptions/profiles/assignments and describe responsibilities for monitoring and reporting suspicious system activity
- RACI guide
- Related description of services provided by involved teams
- SOC team organization structure and responsibilities
- Incident management escalation protocols and responsibilities

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
✓	✓	✓	✓

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

- Responsibility assignments chart (e.g., RACI charts) including key roles such as team lead, communications lead, legal representative, etc.
- Business continuity/resilience policy, standard, and procedures
- Related recovery procedures
- Roles and responsibilities of management and personnel involved in the organization's resilience
- Job descriptions for business management including resilience responsibilities

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
✓	✓	✓	✓

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 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

- Third-party security policy, standard, and procedures
- Third-Party Risk Management Program
- Documentation of roles and responsibilities for Third-Party Risk Management Program
- Related reporting and examples
- Designated third-party engagement managers

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
✓	✓	✓	✓

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

- Organizational structure
- Policies and procedures outlining roles and responsibilities of cybersecurity personnel
- Job descriptions and profiles
- Third-party contracts detailing responsibilities and service level agreements
- Performance related documentation

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
✓	✓	✓	

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

- Asset related processes, roles, responsibilities, and evidence
- Related training for those modifying system of record
- Cybersecurity training schedule and materials
- Job description
- Inventory listings with asset ownership and custodianship designated

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
✓	✓		

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

- Global risk policy
- Policy roadmap
- Description of how the organization develops, implements, and oversees policies, including roles and responsibilities for each process and evidence of segregation of duties (e.g., three lines of defense model)
- Relevant Board and committee (e.g., Steering committee) meeting agendas and minutes
- Organizational charts
- Service catalogs with detailed roles and responsibilities
- RACI Charts demonstrating segregation of duties

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
✓	✓	✓	✓

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

- Relevant Board or committee meeting agendas and minutes
- Relevant Board, committee, and/or senior management approvals of prioritization and resource allocations
- Evidence of changes in program information
- Staff review process, including skills assessment
- Target operating model (i.e., desired state of operations considering the organization's role in critical infrastructure)
- Organizational structure, including clearly defined roles and responsibilities
- Related description of services provided by involved teams
- Legacy systems upgrade and evergreening plans and programs

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
✓	✓	✓	✓

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

- Description of overall budget process, including cybersecurity
- Staff review process, including skills assessment
- Organizational structure, including clearly defined roles and responsibilities

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
✓	✓	✓	✓

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

- Organizational structure
- Relevant Board or committee (e.g., Steering Committee) meeting agendas and minutes where CISO (or designated Cybersecurity Officer) has been on agenda
- Engagement of consultants and professional services
- Documented evidence of strategic planning process and associated resource discussions
- Board approvals
- Related description of services provided by involved teams
- Cybersecurity action plan (layered security approach)
- Description of overall budget process, including cybersecurity
- Approved cybersecurity budget

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
✓	✓	✓	✓

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

- Background/vetting/screening check policy, standards, and procedures
- Metrics of operational effectiveness of policy, standards, and procedures
- Standards or contract clauses for screening of third-party staff

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
✓	✓	✓	✓

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

- Access control policy and procedures covering employee termination
- Termination/leave process to remove access when an employee terminates
- Evidence of access removal within 24 hours of employee's departure
- Evidence of monitoring activities (social media monitoring, data loss prevention, other security monitoring)
- Method and/or process of reporting a violation
- Investigations process
- Evidence of return of assets

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
✓	✓	✓	

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

- Insider threat policy and procedure
- Training related to reporting suspicious activity
- Examples of cybersecurity training and situational awareness campaigns
- Background/vetting/screening check policy, standards, and procedures
- Vetting standard and operating procedures
- List of roles that require additional background checks
- Policies, procedures, and methodologies related to additional background checks for specific roles
- Cyber risk management strategy and framework

Policies, Processes, and Procedures (GV.PO)

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

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.

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

- Technology and Cybersecurity/Information Security Program documentation, including policy, methodology, charters for creating new policies, etc.
- Catalog of approved or ratified policies, or description of which organization/business line within the organization owns and maintains each policy and who approved each policy
- Policy roadmap or process document, including document control to determine if/when policies are reviewed and updated
- Relevant Board and committee meeting agendas and minutes
- Roles and responsibilities of 1LoD and 2LoD

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
✓	✓		

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

- Copies of policies
- Statements or announcements regarding policy and governing body changes/applicability

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
✓	✓	✓	✓

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 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

- Mandatory global risk objectives
- Description of how employees include mandatory global risk objectives in personal performance scorecards
- Technology and cybersecurity training curriculum
- Technology and cybersecurity training for developers
- Technology and cybersecurity situational awareness communications
- Policy citations
- Consequence models in place
- Outcomes of assigned training, such as metrics of staff completed training to comply with requirements
- Evidence of disciplinary action within policy and process for reporting policy violations, consistent with privacy regulations

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
✓	✓	✓	✓

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

- Acceptable use policy, standard, and documentation
- Example of employee handbook acknowledgement
- Training related to acceptable technology, personal device, and social media use
- Policies related to personal device (e.g., BYOD) and social media use

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
✓	✓	✓	✓

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, 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

- Technology and cybersecurity standards, processes, procedures, and controls
- Policy roadmap or process document, including charters for new processes, procedures, and controls
- Evidence that cybersecurity policy aligns with processes, procedures, and controls
- Responsibility assignment matrix/RACI charts

GV.PO-01.06: Physical and environmental security policies are implemented and managed.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

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

- Physical and environmental security policies (may also be called protective security policy), measures, and guidance
- Standards, controls, and procedures supporting implementation of the policy into measurable objectives
- Testing procedures to ensure physical controls are operating as expected (locked doors, server rack cabinets, badge readers, etc.)
- Security logs, visitor access controls, or other measures that demonstrate compliance with policies
- Workplace violence prevention policy

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
✓	✓	✓	✓

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

- Business continuity/resilience policy, standard, and procedures
- Relevant Board and committee meeting minutes and approvals where business continuity and resilience program is discussed

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
✓	✓	✓	✓

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Relevant Board or committee meeting minutes

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.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

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

- Policy roadmap or process document, including document control to determine if/when policies are reviewed and updated
- Cybersecurity policy and standards (including approval and revision history)
- Cybersecurity standards process (including approval and revision history)
- Evidence of risk exceptions to applicable policies
- Communication plan for new and updated policies

Oversight (GV.OV)

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

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.

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, cybersecurity, third-party, and resilience risks. Include examples of information provided to the governing authority.

Examples of Effective Evidence

- Relevant Board or committee (e.g., Board Risk Committee) meeting agendas and minutes
- Risk and control reporting (e.g., risk maps, risk appetite reporting, risk and controls assessment reporting)
- Target operating model (i.e., desired state of operations considering the organization's role in critical infrastructure)

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
✓	✓	✓	✓

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 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

- Relevant Board or committee (e.g., Board Risk Committee) meeting agenda and minutes
- Board reports/presentations and other related meeting agendas/minutes
- Monthly cyber dashboard reporting
- Metric reporting with KPIs and KRIs

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
✓	✓	✓	✓

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

- Key control indicator (KCI) dashboards
- Relevant Board or committee meeting agendas and minutes
- Risk reporting documentation
- Reports related to technology use and risks within the organization

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
✓	✓	✓	✓

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

- Cyber risk management strategy and framework
- Risk appetite statements
- Identification of risk and treatment
- Risk register
- Risk acceptance reports and approvals
- Relevant Board and committee (e.g., Steering committee) meeting agendas and minutes related to residual cyber risk
- Assessment reports that support prioritization of activities to address inherent risk
- Inherent risk analysis documentation
- Threat intelligence reports and analyses

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
✓	✓	✓	

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

- Technology and cybersecurity risk management strategy and framework documentation, including how the organization created the strategy/framework, such as top and emerging risk documentation, risk control assessment, etc.
- Approved risk appetite statements
- Relevant Board and committee (e.g., Steering committee) meeting agendas and minutes related to residual technology and cybersecurity risk
- Specific organization tools/methods for technology and cybersecurity risk quantification
- Control environment and control effectiveness reports
- KRIs, KPIs, and other risk reporting metrics and measures

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
✓	✓	✓	

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 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

- Relevant Board or committee meeting agendas and minutes
- KCI dashboards
- Risk appetite statement, which may include metrics or other measures (e.g., reporting documents/dashboards)
- Relevant Board and committee (e.g., technology and cybersecurity risk strategy committee, steering committee, etc.) meeting minutes and approvals where technology and cybersecurity risk management is discussed
- Monthly cyber dashboards
- Technology and cybersecurity risk management strategy and framework
- Maturity model or methodology used to align KPIs and metrics

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Business continuity/resilience policy, standard, and procedures
- Data center recovery reports and measures
- Service continuity planning reports and measures
- Related recovery measures
- Test results
- Test gaps and proposed remediation
- Tabletop exercise results

Independent Risk Management Function (GV.IR)

TIER 1	TIER 2	TIER 3	TIER 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.

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 the technology and cybersecurity risk management framework, including documentation and evidence of review of credible challenge.

Examples of Effective Evidence

- Risk management framework, including documentation of the risk strategy and risk register that prioritizes risk
- Organization's risk appetite
- Independent risk management function assurance reviews and reports
- Organizational charts to show segregation of risk management function
- Board reporting, including reporting through Chief Risk Officer
- Program management documentation for 2LoD and 3LoD
- Documentation and evidence of review of credible challenge

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
✓	✓	✓	

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).

Examples of Effective Evidence

- Cyber dashboards
- Risk control assessment information and cyber risk events reporting
- Organizational chart
- Risk acceptance program, documents, and tracking
- Risk register
- Relevant Board or committee (e.g., Risk, Risk Management) meeting agendas and minutes
- Organizational chart with reporting lines to demonstrate independence and level of authority
- Documentation and evidence of review of credible challenge

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
✓	✓	✓	

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

- Cyber capability mapping for independent risk management function (all roles)
- Samples of independent function from opinion papers, assurance reviews, challenge papers, etc. to demonstrate understanding of the program, risks, and threats

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
✓	✓	✓	

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

- Risk and control assessments
- Cyber risk events reporting
- Relevant Board or committee meeting agendas and minutes
- 2LoD charter

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
✓	✓	✓	

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

- Relevant Board or committee meeting agendas and minutes
- Independent risk function assessments, reports, or dashboards

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
✓	✓	✓	

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

- Risk Committee charter
- Risk Committee annual review and approval of information security risk program
- Information security risk program supporting information
- Relevant Board or committee meeting agendas and minutes
- Issues tracking/monthly issues review

Audit (GV.AU)

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.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

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

- Internal audit charter(s)
- Audit instruction manual
- Audit policies and procedures
- Contracts for independent audit services

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
✓	✓	✓	✓

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

- Audit instruction manual
- Supporting internal audit plans and reports for cyber-related audit activity
- Control environment reports
- Policies and procedures for updating audit plan

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
✓	✓	✓	✓

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

- Audit instruction manual
- Audit schedule
- Supporting internal audit plans and reports
- Related meeting agenda/minutes

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
✓	✓	✓	✓

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

- Supporting independent (e.g., internal or external) audit plans and reports
- Third-party security policy, standard, and process
- Third-party risk management program
- Documentation of review of the third-party risk management policies and controls
- Relevant Board or committee meeting minutes

GV.AU-01.05: An independent audit function assesses compliance with applicable laws and regulations.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

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

- Audit instruction manual
- Supporting internal audit plans and reports
- Related meeting agenda/minutes

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
✓	✓	✓	✓

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

- Audit instruction manual
- Audit access to independent cyber threat intelligence capability
- Regular audit staff capability assessment
- Audit policies
- Audit plans

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
✓	✓	✓	✓

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

- Audit instruction manual
- Supporting internal audit plans, procedures, and reports
- Audit policies

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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

- Supporting internal audit plans and reports
- Evidence of mitigation (e.g., follow-up reports, routine reviews, updates)

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
✓	✓	✓	✓

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

- Audit instruction manual
- Continuous monitoring reports
- Audit issue tracking reports and escalation criteria
- Issue management policy

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
✓	✓	✓	✓

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

- Internal audit updates and reports (current and previous) to the appropriate governing authority (e.g., Board Audit Committee)
- Internal audit special reports
- Audit issue escalation criteria

CYBER RISK INSTITUTE

IDENTIFY

Asset Management (ID.AM)

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
✓	✓	✓	✓

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

- Asset management policies and procedures
- Asset inventory documentation, including how often inventory is updated to maintain current data, how often it is reviewed and by whom (e.g., by independent risk management, audit), and the inventory method (e.g., automated, manual, or a combination)
- Documentation supporting the operation, mapping, and discovery of assets
- Asset related processes, roles, responsibilities, and evidence
- Related dashboards, inclusive of KRIs / KPIs, on the efficiency and effectiveness of the asset management program
- Related process flows

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
✓	✓	✓	✓

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

- Asset management policies and procedures
- Asset inventory documentation, including how often inventory is updated to maintain current data, and the inventory method (e.g., automated, manual)
- Platform and application review process
- Inventory issue resolution and attestation process documentation
- Design governance documents
- Related dashboards, inclusive of KRIs / KPIs, on the efficiency and effectiveness of the asset management program and related process flow diagrams
- Asset related processes, roles, responsibilities, and evidence

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Data management documentation
- Data management points of contact, including roles and responsibilities
- Inventory reports (e.g., maps of network resources, network diagrams, third-party connections, and mobile resources)
- Operating instructions such as:
  - Remote access management
  - Third-party access management
  - End user security controls
  - System Admin policies/procedures
  - User access guides
  - Information security controls

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
✓	✓	✓	✓

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 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

- Inventory reports which depict external information systems, their key characteristics, and who manages them
- Policies and procedures for maintaining inventory of external hardware, software, and data assets
- Diagrams or connectivity flow documentation
- External systems point of contact information

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
✓	✓	✓	

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

- Related policy and procedure information (e.g., definitions and classifications)
- Data policy inventory
- Data policy governance and oversight meeting agendas and minutes
- Data governance roles and responsibilities (e.g., Privacy Officer, Compliance Officer, etc.)
- Description of tools used to track, update, and report on IT asset inventory
- Documentation of data policy review/evaluation and approval (e.g., quarterly or annually)
- Information classification matrix/guidance for classifying data

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
✓	✓	✓	

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.

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

- Related policy information (e.g., definitions and classifications)
- Business Impact Analysis
- Resource maintenance and upgrade schedules
- Business continuity plans
- Policy governance and oversight meeting agendas and minutes
- Inventory reports
- Description of tools used to track, update and report on IT asset 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
✓	✓	✓	

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

- Data management policies, procedures, and other documentation (e.g., data classification policy)
- Operating guides
- Data quality documentation
- Data flow diagrams
- Operating instructions
- Related training for those modifying system of record
- Related annual document review and approval

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
✓	✓	✓	

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

- Asset inventory
- Data management policies, procedures, and other documentation (e.g., data classification policy)
- Asset management policies and procedures
- Asset related processes, roles, responsibilities, and evidence
- Secure disposal of electronic information policy, standard, and processes, which may include cryptographic destruction
- Secure disposal of physical information policy, standard, and process
- Policies for managing unsupported and end-of-life systems

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
✓	✓	✓	

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. Organizations should employ procurement policies and processes to disallow technology purchases that have not been appropriately reviewed and approved.

Examples of Effective Evidence

- Related tools
- Cybersecurity training curriculum inclusive of shadow IT risks
- Asset management policies and procedures
- Asset inventory documentation, including how often inventory is updated to maintain current data, how often it is reviewed and by whom (e.g., by independent risk management, audit), and the inventory method (e.g., automated, manual, or a combination)
- Documentation supporting the operation, mapping, and discovery of assets
- Asset related processes, roles, responsibilities, and evidence
- Procurement and contracting policies and procedures

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

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.

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

- Data management policies, procedures, and other documentation (e.g., data classification policy)
- Data policy inventory
- Data policy governance and oversight meeting agendas and minutes
- Data governance roles and responsibilities (e.g., Privacy Officer, Compliance Officer, etc.)
- Data retention policy, standard, and procedures
- Data retention schedules
- Data center data destruction procedures
- Data destruction agreements with third parties, including attestation of data destruction
- Data lifecycle management documentation

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
✓	✓	✓	✓

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

- Information asset security policy
- Asset inventory
- Secure disposal of electronic information policy, standard, and processes, which may include cryptographic destruction
- Secure disposal of physical information policy, standard, and process
- Evergreening policy, standard, and process
- Mobile device management procedures for lost mobile devices

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
✓	✓	✓	✓

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

- Data retention policy, standard, and procedures
- Data retention schedules
- Data center data destruction procedures
- Data destruction agreements with third parties, including attestation of data destruction

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
✓	✓	✓	✓

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract guidance
- Contract clauses
- Contract reporting
- Data return/destruction policies and procedures
- Certificate of destruction

Risk Assessment (ID.RA)

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Risk management frameworks and process documentation
- Risk and control assessments and results
- Various risk committee meeting agendas and minutes
- Participation in cyber exercises, and related assessments of risks and vulnerabilities and action items

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
✓	✓	✓	✓

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

- KRIs and KPIs, metric reporting, dashboards, or presentations provided to senior management
- Documents on senior management response to metrics, dashboards, presentations
- Risk management framework
- Policies and procedures for risk acceptance escalation
- Committee meeting agendas and minutes
- Risk and control assessments and reporting
- Corporate and business units risk strategy
- Remediation reports

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Vulnerability management security standards and procedures, including eligibility
- Risk assessment criteria
- Related tools
- Applications and supporting infrastructure security testing policies, standards, and procedures
- Related reporting (dashboards)
- Remediation/patching processes
- Evidence of asset reconciliation procedures to ensure comprehensive testing is completed against all environments
- Risk acceptances for patches on systems, applications, etc.
- Evidence of application security testing, including Web-based applications connected to the Internet, against known types of cyber attacks (e.g., SQL injection, cross-site scripting, buffer overflow) before implementation or following significant changes
- Evidence of independent penetration testing of network boundary and critical Web-facing applications is performed routinely to identify security control gaps

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.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

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).

Examples of Effective Evidence

- List of information-sharing groups and collectives in which the organization participates across the globe
- Cyber threat reports
- Cyber intelligence and threat analysis and alerts
- Procedures for gathering, distributing, and analyzing threat information
- Procedures for sharing information with external parties
- Participation in exercises and related action items
- Related agendas and meeting minutes

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
✓	✓	✓	

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.

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

- Security incident response policies, standards, procedures, and communication templates
- Cyber threat and resilience information sharing examples
- Evidence of membership in industry associations and/ or information sharing organizations
- Information sharing examples
- Maturity documentation for protective measures

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
✓	✓	✓	✓

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

- Cyber threat identification, documentation, analysis and response policies and procedures
- Cyber threat intelligence and threat analysis reports
- Cyber risk assessment documentation
- Other related cyber threat assessments
- Threat catalogs

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
✓	✓	✓	✓

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

- Cyber threat intelligence policies and standards
- Vulnerability standards
- Patch management policies and standards
- Cyber threat intelligence reporting
- Cyber incident reporting
- Control environment meeting agendas and minutes
- Risk assessment processes
- List of staff and organization memberships
- Threat catalog
- Customer notifications about how to report suspected cyber issues

ID.RA-03.03: The organization includes in its threat analysis those cyber threats which could trigger extreme 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
✓	✓	✓	

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

- Cyber threat response policies and procedures
- Cyber intelligence and threat analysis reports and alerts
- Related cyber threat assessments and controls for mitigation assessment
- Control assessments
- Tabletop exercises (e.g., exercises that included extreme but plausible cyber events as vignettes)
- Business impact assessment
- Threat catalogs

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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

- Cyber threat reports and alerts
- Cyber intelligence and threat analysis reports and alerts
- Examples of periodic updates/reporting on cyber threats
- Cyber threat assessments and control environments
- Vulnerability and penetration testing reports
- Tabletop exercises and action items
- Related threat intelligence tools
- Red team/purple team testing documentation, including plans, and resulting reports
- Threat catalogs

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
✓	✓	✓	✓

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

- Business impact assessments
- Risk assessment methodology
- Operational risk management framework
- Risk and control assessments
- Application security reviews
- Third-party security reviews
- Independent risk and residual risk likelihood and impact reports

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
✓	✓	✓	✓

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

- Operational risk framework
- Risk reporting
- Overall assessments of cyber risk to the organization
- Impact assessments
- Risk assessment methodology
- Enterprise risk strategy
- Subscription to threat intelligence feeds that inform the organization of changing threat condition over time

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
✓	✓		

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.

Examples of Effective Evidence

- Cyber threat intelligence reporting
- Threat scenario assessments
- Threat modeling process documentation
- Threat catalog
- Threat models utilized within the organization
- Inventory of all critical assets
- Controls and security assessments on critical assets
- Documentation of tabletop exercises and action items

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
✓	✓	✓	

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

- Risk and control assessments, including documentation of design and scope
- Risk strategy reports
- Risk impact reports
- Risk register

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
✓	✓	✓	

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

- Security incident response policies, standards, and procedures
- Tabletop exercises and/or simulations
- Use cases
- Related assessment reporting
- List of applicable use cases or scenarios for test cases

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
✓	✓	✓	✓

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

- Risk assessments (e.g., the Profile, NIST, the FFIEC Cybersecurity Assessment Tool (CAT), external third-party risk assessment)
- Issue tracking reports
- Audit reports
- Relevant Board and committee meeting agendas and minutes
- Risk management meeting agendas and minutes
- Communications regarding issues and findings between cyber risk identification and remediation teams
- Remediation activity logs

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
✓	✓	✓	✓

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

- Risk acceptance and risk exception procedures
- Risk management framework
- Reviews demonstrating risk acceptance standard is followed (e.g., application and system security reviews, security testing standard for applications and infrastructure, etc.)
- Cyber and business insurance documentation
- Risk assessment methodology
- Communications regarding issues and findings between cyber risk identification and remediation teams
- Remediation activity logs

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
✓	✓	✓	✓

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

- Related reports regarding governance of the control environment
- Related independent assurance reviews on specific control topics/overall programs of work
- Risk appetite statements
- Identification of risk and treatment
- Risk acceptance reports and approvals
- Risk register

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
✓	✓	✓	✓

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

- Business impact assessments
- Tabletop exercises (e.g., exercises that included extreme but plausible cyber events as vignettes)
- Business continuity/resiliency plans, policies, and procedures
- Recovery time objectives
- Recovery point objectives
- Business continuity/resilience policy, standard, and procedures

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
✓	✓	✓	✓

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

- Vulnerability management security standards and processes
- Remediation/patching processes
- Metrics and reporting used
- Exception management processes
- Remediation reports or metrics with timelines
- Risk acceptances for patches on systems, applications, etc.
- Related reporting (dashboards)

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
✓	✓	✓	✓

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

- Security incident response policies, standards, and procedures
- Incident response examples and playbooks
- Vulnerability management security policy, standard, and procedures
- Mitigation management policy, standard, and procedures
- Risk acceptance policy, standard, and procedures
- Exception management procedures

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
✓	✓	✓	✓

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

- Secure system development standard
- Security testing standard for applications and supporting infrastructure
- Change management policy, standard, and process, including:
  - Risk evaluation
  - Formal approval processes
  - Implementation and backout test plans
- Control indicator reporting
- Change advisory boards meeting minutes
- Related documentation (e.g., possibly change tickets)
- Project management standards and procedures

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
✓	✓	✓	

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

- Change management policy, standard, and process, including:
  - Risk evaluation
  - Formal approval processes
  - Implementation and backout test plans
- Secure system development standard
- Security testing standard for applications and supporting infrastructure
- Related documentation (e.g., possibly change tickets)
- Change advisory boards meeting minutes

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
✓	✓	✓	

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, 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

- Secure system development standard
- Change management policy, standard, and process
- Secure system development standard
- Related documentation (e.g., possibly change tickets)
- Project management standards and procedures
- Business continuity/resilience plans and procedures

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
✓	✓	✓	

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

- Risk acceptance policy, standard, and procedures
- Risk acceptance/exception management process
- Required approvals
- Evidence of mitigation (e.g., follow-up reports, routine reviews, updates)
- Cyber-related reviews demonstrating risk acceptance standard is followed (e.g., application and system security reviews, security testing standard for applications and infrastructure, etc.)
- Risk management framework
- Cyber risk assessment methodology
- Audit issue tracking reports and escalation criteria
- Evidence of risk exceptions to applicable policies

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
✓	✓	✓	✓

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

- Risk acceptance/exception management process
- Required approvals
- Risk acceptances for delay to patches on systems, applications, etc.
- Documentation of any network segmentations and VLANS
- Related reporting (dashboards)
- RACI matrix for exception management
- Standards and procedures for the management of unsupported or end-of-life systems

ID.RA-08.01: The organization has established enterprise processes for soliciting, receiving and appropriately channeling vulnerability disclosures from:

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

(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).

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

- Vulnerability management security standard
- Cyber threat reporting and intelligence examples
- Cyber threat analysis examples
- Organizational structure
- Related description of services provided by involved teams
- Related job profiles
- Group distribution lists
- Related collaboration and information sharing examples
- Contractual information sharing agreements

ID.RA-08.02: The organization has established enterprise processes to analyze disclosed vulnerabilities with a focus on:

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

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.**

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

- Vulnerability management security standard
- Remediation management documentation
- Relevant Board and committee meeting agendas and minutes
- Related reporting
- Cyber threat analysis examples
- Related collaboration and information sharing examples
- Exception management procedures

Improvement (ID.IM)

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
✓	✓	✓	✓

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

- Applicable assessment results
- Testing procedures to ensure technology, cybersecurity, and resilience controls are operating as expected
- Evidence of testing performed routinely to identify security control gaps

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
✓	✓	✓	

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

- KCI/KPI/KRI dashboards
- Risk appetite statement, which may include metrics or other measures (e.g., reporting documents/dashboards)
- Relevant Board or committee meeting agendas and minutes
- Process for modifying/maintaining KCIs/KPIs/KRIs
- Maturity model or methodology used to align KPIs and metrics

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
✓	✓	✓	

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 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

- Risk management framework, including documentation of the risk strategy and risk register that prioritizes risk
- Risk appetite statement(s), which may include metrics or other measures (e.g., reporting documents/dashboards)
- Risk identification process available to all staff (open risk culture)
- Risk reporting documentation
- Key control indicator (KCI) dashboards
- Relevant Board or committee meeting agendas and minutes

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Relevant Board or committee meeting agendas and minutes
- Project management standards for quality management
- Quality program standards and procedures

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Enterprise risk management framework documentation
- Operational risk management framework documentation
- Third-party security policy, standard, and process
- Third-party risk management program
- Documentation of review of the third-party risk management program
- Documentation showing resiliency testing in conjunction with external suppliers

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
✓	✓	✓	✓

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

- Security testing for applications and supporting infrastructure policies, standards, and procedures
- Vulnerability management security policies, standards, and procedures
- Proof that penetration testing tools and processes are independent and conducted according to the risk assessment for external facing systems
- Red team tools and processes
- Copy of penetration tests along with remediation plans
- Related reporting (e.g., issues, lessons learned, final report, etc.)
- Proof that testing is conducted at least annually and based upon changes to the environment and risk identification

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
✓	✓	✓	

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

- Vulnerability and penetration testing reports
- Red team/purple/blue team testing documentation, including plans, and resulting reports
- Penetration testing tools and processes

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
✓	✓	✓	

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

- Security incident response policies, standards, and procedures
- Documented cybersecurity incident response plan testing that occurs at least annually
- Test plans applicable to business continuity/disaster recovery
- Escalation and communication plans
- Metrics and reporting of – tabletop exercises, calling trees, and business continuity exercises
- Applicable assessment results (generated by the organization or a third party)
- Verify run books
- Related governance reporting

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
✓	✓	✓	✓

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

- Business continuity/resiliency plans, policies and procedures
- Network penetration testing strategy
- Application security testing strategy
- Data recovery testing
- Targeted test results and reports
- Security assessments
- Results of testing exercises, including metrics or board reporting
- Evidence of testing critical online systems and processes to withstand stresses for extended periods (e.g., DDoS)
- Evidence that testing involves collaboration with critical third parties
- Evidence that testing is comprehensive and coordinated across all critical business functions
- Evidence of all tests conducted in the past 12 months for business continuity / disaster recovery

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
✓	✓	✓	✓

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

- Business continuity/resiliency plans, policies, and procedures
- Roles and responsibilities for staff involved in resumption of critical operations
- Evidence of tabletop exercises or other testing programs
- Business continuity / disaster recovery exercises that were conducted in the past 12 months
- List of applicable use cases or scenarios for test cases
- Business impact analysis and business continuity management risk analyses
- Internal and external dependency analyses

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.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

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

- Business continuity/resiliency plans
- Risk management frameworks and process documentation considering likely recovery scenarios and impact to data integrity, data loss and availability
- Information classification
- Service continuity planning policy, standards, and processes
- Related testing results and reports
- Incident response plan
- Articulation of participation in industry-wide back-up methodologies such as the Sheltered Harbor program within the FS-ISAC

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
✓	✓		

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

- Business continuity/resiliency plans, policies, and procedures
- Roles and responsibilities of organization's governing body
- Executive Committee engagement documentation, agenda, and/or minutes
- Incident management program
- Organizational chart for crisis management
- Applicable working group meetings along with meeting minutes
- Tabletop exercises

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
✓			

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

- Security incident response policy, standard, and procedures
- Business continuity/resilience policy, standard, and procedures
- Related response plan detail
- Related test summaries and reports

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
✓	✓	✓	

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

- Related testing results and reports
- Incident response plan
- Evidence of retesting performed to validate
- Risk acceptance/exception management process
- Required approvals

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
✓	✓	✓	✓

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

- Security incident response standard, process, and plans
- Related tools and industry mapping
- Project charter or plans for updating and enhancing processes
- Change management documentation applicable to enhancing processes
- Evidence of incorporation of lessons learned into cybersecurity defenses such as:
  - Phishing exercises / employee awareness programs
  - Real-life cyber incidents and attacks
  - Independent audits, red team or purple team exercises
- Benchmarks or target performance metrics to show improvements or regressions of the security posture over time

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
✓	✓	✓	

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

- Security incident response policies, standards, and procedures
- Cybersecurity incident response plan example
- Threat and vulnerability intel alert examples are used to enhance internal risk management and controls
- Lessons learned documentation or other related evaluation and assessment documents
- Third-party and/or internal audit reports
- Use cases
- Proof of processes for identifying additional expertise needed to improve information security defenses
- Scenarios used to improve incident detection and response
- Proof that detection processes are continuously improved

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
✓	✓	✓	✓

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.

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

- Policies, standards, plans, and procedures that relate to business continuity, resiliency, disaster recovery planning, crisis management, and incident response
- Recent business impact analysis
- Organizational information
- List of essential staff members, including roles and responsibilities
- Related tabletop exercises
- Stress tests of infrastructure and services
- Run books for business continuity / disaster recovery

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
✓	✓	✓	✓

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

- Security incident response policies, standards, and procedures
- Responsibility assignments chart (e.g., RACI charts) including key roles such as team lead, communications lead, legal representative, etc.
- Business continuity/resilience policy, standard, and procedures

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
✓	✓		

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.

Examples of Effective Evidence

- Data center recovery procedures
- Service continuity planning standards and procedures
- Business continuity/resilience policy, standard, and procedures
- Related recovery procedures
- Third-party service level agreements and contracts

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
✓	✓		

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

- Risk management frameworks and process documentation
- Information classification
- Data center recovery procedures
- Backup and restore standards inclusive of recovery time objectives (RTO) and recovery point objectives (RPO)
- Backup and restore testing standards and processes
- Related testing documentation
- Service continuity planning standards, processes, and plans
- Business continuity/resiliency plans

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
✓	✓		

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

- Data center recovery procedures
- Service continuity planning standards and procedures
- Business continuity/resilience policy, standard, and procedures
- Related recovery procedures
- Key indicator and trigger monitoring reports

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
✓			

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.

Examples of Effective Evidence

- Cyber information sharing
- Related reporting
- Related committee meeting agendas and minutes
- Risk assessment examples

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Security incident response policies, standards, and procedures
- Roles and responsibilities (i.e., forensics, root cause analysis teams)
- Contracts or retainer agreements for forensic investigation expertise

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:

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

(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.**

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

- Security incident response policy, standard, and procedures
- Incident response examples or playbooks
- Cyber analysis and reporting
- Related standards and processes

CYBER RISK INSTITUTE

PROTECT

Identity Management, Authentication, and, Access Control (PR.AA)

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Access control policy and related procedures
- Role-based access control standard and procedures
- Password/pin management standard
- Access request process
- Risk-based periodic access review
- Other assessments of applications or systems validating compliance with access control policy and related procedures, such as use of password vaulting applications to control privileged credentials

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
✓	✓	✓	✓

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

- Access control, request, and review security standards and policy
- Physical security assessment results and other related reports
- Physical access logs and entrance approval lists
- Access approval document (monthly, quarterly, annually)
- Entitlement review reports
- Physical access controls for network ports, collaborative computing devices, and applications
- Related training

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
✓	✓	✓	✓

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

- Identity access management policy, standards, and procedures
- Identification and authentication policy, standards, and procedures
- Network access control standards and procedures
- Access request and review security standard and procedures
- Access control security standard
- Password/PIN management standards
- Role based access control documentation
- Sample requests
- Call center authentication procedures

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
✓	✓	✓	✓

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

- Authentication security policy, standard, and procedures
- Identification and authentication policy, standards, and procedures
- Service level management standard
- Privileged access policy, standard, and procedures
- Third-party access policy, standard, and procedures
- Real-time risk prevention or mitigation tactics
- Application/service access risk assessment

PR.AA-03.02: Decisions to authorize user access to devices and other assets are made with consideration of:

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

(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.

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

- Risk assessment methodologies utilized and samples of completed ones
- Oversight reports showing completion of assessments
- Access request and review security standard and procedures
- Secure remote working information
- Security standards
- Data classification standard
- Third-party assessment process
- Endpoint exceptions
- Computer system access control policy, standard, and procedures
- Remote connectivity security policy, standard, and procedures
- Authentication security policy, standard, and procedures
- Network security diagrams, security architecture, etc.

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
✓	✓	✓	✓

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

- Proof that email protection mechanisms are used to filter for common cyber threats (e.g., attached malware or malicious links)
- Managing electronic information policies, standards, procedures
- Email server security standards

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
✓	✓	✓	✓

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). Describe authorization mechanisms that are implemented and designed to maintain security, integrity, and authenticity.

Examples of Effective Evidence

- Access request process
- Risk-based periodic access review
- Computer system access control policy, standard, and procedures
- Inventory and ownership of service accounts
- Periodic review of access authorization documentation and password refresh
- Proof that authorization mechanisms are implemented for internal systems and across security perimeters
- Third party connection authorization documentation

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Access policy, standard, and procedure
- Segregation of duties security standard
- Role based access control information
- Support documentation and samples
- Privilege user entitlement reviews
- Third-party access policy, standard and procedure

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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.

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

- Privileged access policy, standard, and procedure
- Committee meeting agendas and minutes supporting the topic
- Privileged account management system documentation and procedures
- Privileged account monitoring and alerting procedures
- Periodic review of access authorization documentation
- Evidence that administrators have two accounts; one for administrative use and one for general purpose
- Evidence of controls to prevent unauthorized escalation of user privileges such as software installation

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Computer system access control policy, standard, and procedures
- Access request and review security standard
- System hardening standards
- Application whitelisting tools and procedures
- Privileged access policy, standard, and procedure
- Service account policy
- Inventory and ownership of service accounts
- Periodic review of access authorization documentation and password refresh
- Third party connection authorization documentation

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
✓	✓	✓	✓

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Documentation of roles and responsibilities for external dependencies
- Documentation on contract language that permits monitoring of third-party access
- Related reporting and examples

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
✓	✓	✓	✓

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

- Physical access controls policy
- Related logs
- Sensitive area access process documentation
- Physical security access recertification documentation
- Access request and review security standard
- Use of equipment and systems documentation
- Protection of off-premises equipment documentation (e.g., full disk encryption for laptops or thumb drives)

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
✓	✓	✓	✓

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

- Physical access controls policy
- Security logs, visitor access controls, or other measures that demonstrate compliance with policies
- Sensitive area access process documentation
- Physical security access recertification documentation
- Access request and review security standard
- Use of equipment and systems documentation
- Related training
- Protection of off-premises equipment documentation (e.g., full disk encryption for laptops or thumb drives)

Awareness and Training (PR.AT)

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
✓	✓	✓	✓

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 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

- Information and cybersecurity risk policy, standards, and procedures
- Cybersecurity training standards, schedule, materials, and records (including metrics)
- Job-relevant or job-specific cybersecurity training
- Examples of cybersecurity training and situational awareness campaigns
- Training records

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
✓	✓	✓	✓

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

- Information and cybersecurity risk policy, standards, procedure
- Policy and procedure on reporting cyber incidents or unusual cyber activity
- Cybersecurity training schedule, materials, and records, including timeframe training occurred (e.g., completion metrics)
- Cybersecurity training materials and records (e.g., completion metrics) provided by third parties, if applicable
- Third-party cybersecurity training policy, standards, and procedures
- Examples of training

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
✓	✓	✓	✓

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

- Risk assessment
- Security policies and standards
- Cybersecurity training schedule and materials (including process for reviews and updates)
- Training-related description of services provided by training team
- Examples of training
- Linkage between identified risks and training curriculum

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
✓	✓	✓	✓

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

- Job-relevant or job-specific cybersecurity training
- Examples of cybersecurity training related to new technology
- Cybersecurity training schedule, materials, and records, including timeframe training occurred (e.g., completion metrics)
- Cybersecurity training materials and records (e.g., completion metrics) provided by third parties, if applicable
- Project change management plans

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Cybersecurity training schedule, materials, and evidence of completion
- Training-related description of services provided by training team
- Certification requirements for cybersecurity personnel
- Training and development plans
- Review of training hours and effectiveness of training related to cybersecurity
- Evidence of professional certifications, if applicable
- Independent review of existing security capabilities and expertise
- Examples of training

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
✓	✓	✓	✓

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 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

- Cybersecurity training schedule and materials (including training provided to management)
- Updated and maintained training-related description of services provided by training team
- Examples of training

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
✓	✓	✓	✓

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

- Security incident response policies, standards, and procedures
- Incident response examples or playbooks
- Documentation of testing (i.e., tabletop exercises) demonstrating roles and responsibilities
- Related description of services provided by involved teams
- Documentation on the communication of incident response information, including roles and responsibilities, to stakeholders
- Escalation policies that address when different personnel within the organization will be contacted and the responsibility those personnel have in incident analysis and response

CYBER RISK INSTITUTE

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
✓	✓	✓	

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 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

- Certification requirements for cybersecurity personnel
- Cybersecurity training schedule and materials (including training provided to management)
- Updated and maintained training services provided by training team
- Examples of incident management and forensic investigation training
- Review of training hours and effectiveness of training
- Certification requirements for cybersecurity personnel
- Training and development plans

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
✓	✓	✓	✓

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

- Third party cybersecurity training schedule, materials, and records, including timeframe training occurred (e.g., completion metrics)
- Third party cybersecurity training materials and records (e.g., completion metrics)
- Examples of third party training

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
✓	✓	✓	✓

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

- Samples of any documentation or website materials that support customer awareness communication programs
- Samples of email and social media programs / documentation
- Annual review of customer awareness training

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:

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

(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.

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

- Cybersecurity training documents
- Cybersecurity situational awareness materials
- Training and situational awareness delivery schedule
- Related training material and samples
- Director education materials related to information and cybersecurity
- Relevant Board or committee meeting minutes and agendas that discuss cybersecurity expertise
- Training scenarios or exercises
- Evidence of completion of training by governing body and senior management

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
✓	✓	✓	✓

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

- Board Director education materials related to information security and cybersecurity
- Relevant Board or committee meeting minutes and agendas that discuss cybersecurity expertise
- Organizational charts

Data Security (PR.DS)

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
✓	✓	✓	✓

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

- Data classification and protection policy
- Physical and environmental information security policy
- Managing electronic information security standard
- Cryptography and key management standard
- Password/PIN management security standard
- Data-at-rest security documentation
- Mobile device standards (laptop, removable media)
- Evidence that data is encrypted
- Data inventory

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
✓	✓	✓	

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

- Data leakage prevention operations guide
- Data leakage prevention monitoring
- Security incident response policy, standard, plan, and process
- Privileged access security standard
- Device permissions standard
- Related tool documentation
- Network security standard
- Behavioral analytic and rate limiting tools
- Tool catalog

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
✓	✓	✓	✓

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

- Removable storage devices policy, standard, procedure
- Mobile/communication devices policy, standard, and procedure
- Related tools, examples, and reporting
- Container controls/tools
- Bring your own device (BYOD) user agreements
- Evidence of endpoint protections preventing unauthorized use of removeable media and control standards enforcing appropriate use (e.g., encryption of removable media)
- Evidence that antivirus and anti-malware tools are deployed on end-point devices (e.g., workstations, laptops, and mobile devices) and include configurations appropriate to removable media (scanning USB drives, CD/DVD upon connection, prevent boot to removable media)
- Access control procedures for removable media

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
✓	✓	✓	✓

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

- Information classification policy
- Managing electronic Information security standard
- Secure transfer of electronic Information
- Secure use of removable storage devices
- Network security standard
- Encryption guide
- Transport Layer Security (TLS) and SecureMail Description
- Messaging security standard
- File transmission security standard
- Data-in-transit demonstrating encryption

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

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.)

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 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

- Data-in-use security documentation
- Evidence that data is encrypted
- Data classification and protection policy
- Physical access controls for network ports, collaborative computing devices, and applications
- Access control policy and related procedures
- Password/pin management standard
- Access request process
- Risk-based periodic access review

CYBER RISK INSTITUTE

TIER 1	TIER 2	TIER 3	TIER 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.

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

- Risk management frameworks and process documentation
- Information classification
- Data backup and recovery policy, standard, and process
- Backup and restore standards and plans, inclusive of critical applications
- Backup and restore testing standards and process
- Formal backup and recovery testing documentation
- Documentation evidencing annual tests of systems, applications, and data recovery
- Data/system recovery time objectives, recovery point objectives, and impact tolerance requirements

Platform Security (PR.PS)

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
✓	✓	✓	

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

- Anti-virus and anti-malware control documentation
- Monitoring dashboard reports comparing baselines against current configurations
- Related security policies, standards, and procedures
- Related configuration policies, standards, and procedures
- Procedures relating to the use of centralized configuration management tools
- List of baselines
- Sample of baselines, including use/reference to industry standards or vendor recommendations

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
✓	✓	✓	✓

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.[13] 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

- System configuration policy, standard, and procedure
- Standard build documentation
- System monitoring reports
- Access and authentication controls
- Evidence of boundary device (firewall, router, intrusion detection systems (IDS) / intrusion prevention systems (IPS)) rule review, audit, and updates

[13] NIST Special Publication 800-53, CM-7 Least Functionality and ISO 27001 A.12.5.1 "Installation of Software on Operational Systems".

CYBER RISK INSTITUTE

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 rectified.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

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

- Software management security standard
- Security baseline processes and procedures
- Procedures for file integrity monitoring
- Related tool and frequency documentation
- Monitoring dashboard reports
- Remediation management documentation
- Routine rotation of devices with known clean images

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
✓	✓	✓	✓

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 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

- Documents describing the organization's business, technical, and security requirements for authoritative time sources, time accuracy and synchronization
- Design documents reflecting the organization's time synchronization infrastructure, network flows, and services, to include redundant service components
- Operations and maintenance documentation for time synchronization infrastructure and services
- Hardware and software configuration standards for the synchronization of system clocks
- Evidence of time solution testing (e.g., control test results, tabletop exercise results, disaster recovery test results)

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
✓	✓	✓	✓

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

- Encryption standards, methods, and management practices, including evidence of consistency with industry standards
- Evidence of a process in place to modify the standards, methods, and/or practices due to changes in international, national, and financial services industry standards and guidelines

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Cryptography and key management standard
- Cryptographic algorithms standard
- Encryption systems and key management documentation
- Cyber risk management strategy and framework
- Information classification policies, standards, procedures

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
✓	✓	✓	✓

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

- Cryptography and key management standard
- Cryptographic algorithms standard
- Third party connection standards
- Third party environment security standards (e.g., cloud environment standards)

TIER 1	TIER 2	TIER 3	TIER 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.

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

- Inventory reports which depict external information systems, their key characteristics, and who manages them
- Policies and procedures for maintaining inventory of external information systems
- Diagrams or connectivity flow documentation
- Evidence of mechanisms implemented to protect network, application, and data integrity
- End user device protection software selection
- End user device software configuration standards

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
✓	✓	✓	✓

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

- Data leakage prevention operations guide
- Data leakage prevention monitoring
- Mechanisms employed related to restricted access, locking-down device source network locations, etc.
- Evidence of multi-factor authentication
- Virtual endpoint software configuration standards

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Patch management policy, standard, and process
- Criticality assessment evaluation criteria and process
- Communication strategy for notification of necessary patches
- Tooling
- Related reporting (dashboards, logs, etc.)

CYBER RISK INSTITUTE

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
✓	✓		

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 changes and new functionality. Describe the policies and practices used to address unsupported and end-of-life applications.

Examples of Effective Evidence

- System Development Life Cycle (SDLC) policy, standards, practices, and procedures
- Application security processes and procedures including testing for common vulnerabilities (OWASP), code integrity
- System development lifecycle documentation
- Related development documentation
- Developer training documentation
- Source code analysis processes and procedures
- Application change request process
- Policies to address unsupported or end-of-life applications

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
✓	✓	✓	

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

- System Development Life Cycle (SDLC) policy, standards, practices, and procedures
- Application security processes and procedures including testing for common vulnerabilities (OWASP), code integrity
- System development lifecycle documentation
- Related development documentation
- End-of-life decommissioning processes and standards
- Evidence of risk-based planning

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
✓	✓	✓	

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

- Related policies, standards, and process (e.g., data center access, equipment maintenance, retiring of assets, and destruction of components)
- Control environment around these processes
- Monitoring dashboards
- Inventory of assets
- Asset maintenance logs or other metrics
- Remote connectivity security standard
- Privileged access security policy, standard, and process
- Specific procedures related to vendor maintenance of assets
- Related policies and procedures
- Roles and responsibilities
- Access request and review process

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
✓	✓	✓	✓

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

- Security event logging and monitoring policy, standard, and procedure
- Evidence of log review for adequacy of log content, device reporting, and testing of alerting functionality

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.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

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

- Security event logging and monitoring policy, standard, and procedure
- Evidence of log review for adequacy of log content, device reporting, and testing of alerting functionality

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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

- Security event logging and monitoring policy, standard, and procedure
- Data retention policy, procedure, and standard
- Examples of tools used
- Related procedure documents
- Evidence of logs and configuration settings matching log retention documentation
- Evidence of segregation of access between logging sources and storage location

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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

- Anti-malware security standards and procedures
- Proof that anti-virus and anti-malware tools are deployed on end-point devices (e.g., workstations, laptops, and mobile devices) and used to detect attacks
- Forensic security standards and procedures
- Proof that mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks
- Proof that up-to-date antivirus and anti-malware tools are used
- Related reporting to management
- Proof that programs that can override system, object, network, virtual machine, and application controls are restricted

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
✓	✓	✓	✓

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

- Removable storage device policies, standards, and procedures
- Mobile device security policies, standards, and procedures
- Managing electronic information policies, standards, and procedures
- Storage security policies, standards, and procedures
- Related patch deployment policies, standards, and procedures
- BYOD policies, standards, and procedures
- Proof that anti-virus and anti-malware controls are in place to detect attacks and alert management.

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
✓	✓	✓	✓

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

- Information classification policies, standards, procedures
- Managing electronic information policies, standards, procedures
- Email server security standards
- Proof that email protection mechanisms are used to filter for common cyber threats (e.g., attached malware or malicious links)
- Messaging system security standards
- Anti-malware security standards
- Other related policies, standards, and procedures
- Anti-virus and anti-malware controls
- Proof that antivirus and anti-malware tools are used to detect attacks
- Training examples and attestation
- Tool examples
- Related reporting
- Procedures for updating malware signatures and behavior patterns

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
✓	✓	✓	

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 secure-by-design methodologies and vendor recommendation during all phases of both traditional and agile projects.

Examples of Effective Evidence

- Application security processes and procedures including testing for common vulnerabilities (OWASP), code integrity
- System development lifecycle documentation
- Related development documentation
- Developer training documentation
- Source code analysis processes and procedures
- DevSecOps processes and procedures
- Platform environment specific development standards and practices

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
✓	✓	✓	

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

- Secure system development standards and processes, including how cybersecurity risk is incorporated during the beginning of processes
- Security testing standards, processes, and reports
- Other related policies, standards, and procedures
- Platform/environment specific secure SDLP standards & practices
- DevSecOps practices and procedures

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
✓	✓	✓	

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

- Secure system development standards and processes
- System development lifecycle documentation
- Evidence of fundamental, operational, resilience, and security requirements
- Related SDLC tracking/management documentation
- Stakeholder approvals and/or SDLC meeting minutes
- Requirements traceability matrices

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
✓	✓	✓	

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

- Application security processes and procedures including testing for common vulnerabilities (OWASP), code integrity
- System development lifecycle documentation
- Evidence of implemented security mechanisms for system development and testing tools, processes, and environments

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
✓	✓	✓	

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

- Security testing standard for applications
- Related testing documentation
- Migration activities
- Application security processes and procedures including testing for common vulnerabilities (OWASP), independent code review and code integrity
- System development lifecycle documentation
- Related development documentation
- Developer training documentation
- Source code analysis processes and procedures
- Platform/environment specific testing tools and 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
✓	✓	✓	

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

- Security testing standard for applications
- Related testing documentation
- Application security processes and procedures including testing for common vulnerabilities (OWASP), independent code review and code integrity
- System development lifecycle documentation
- Related development documentation
- Developer training documentation
- Source code analysis processes and procedures
- Vulnerability exception management process

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
✓	✓		

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

- DevOps/DevSecOps practices and procedures
- Security testing standard for applications
- Related testing documentation
- Application security processes and procedures including testing for common vulnerabilities (OWASP), independent code review and code integrity
- System development lifecycle documentation
- Related development documentation
- Developer training documentation
- Source code analysis processes and 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
✓	✓		

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 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

- Related configuration policies, standards, and procedures
- Procedures relating to the use of centralized configuration management tools
- System development lifecycle documentation
- Related development documentation
- System user guides, operations, documentation, etc.

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
✓	✓		

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.) 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

- Related models
- Security testing standard for applications
- Related testing documentation
- Application security processes and procedures including testing for common vulnerabilities (OWASP), independent code review and code integrity
- System development lifecycle documentation
- Related development documentation
- Developer training documentation
- Source code analysis processes and procedures
- Critical business model and end-user computing inventory

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
✓	✓	✓	

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

- Related security policies, standards, and procedures
- Related configuration policies, standards, and procedures

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
✓	✓		

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 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

- KPI dashboards
- Relevant stakeholder meeting agendas and minutes
- KPIs, metric reporting, dashboards, or presentations provided to stakeholders
- Related policies, standards, and procedures
- Evidence of functions being tracked and monitored

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
✓	✓		

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

- Stakeholder meeting agendas and minutes
- Related performance indicators (requirements, SLAs, OLAs)
- Related reporting documentation
- IT service catalogs
- IT service request processes and supporting tools

Technology Infrastructure Resilience (PR.IR)

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
✓	✓	✓	✓

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.

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

- Network perimeter security policy, standard, and procedures describing separate trust/security zones
- Internal corporate network security policy, standard, and procedures describing separate trust/security zones
- Network management policy, standard, and procedures
- Mobile device security standard
- Related framework and strategy documents
- Network security diagrams, security architecture, etc.

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
✓	✓	✓	✓

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

- Network device baseline configuration documents
- Monitoring dashboard reports comparing baselines against current configurations
- Related network device configuration policies, standards, and procedures
- Procedures relating to the use of centralized configuration management tools

CYBER RISK INSTITUTE

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
✓	✓	✓	

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

- Internal network security standard
- Network management standards
- Network perimeter security standard
- Other related policies, standards, and procedures
- Risk assessments
- Tools and controls examples
- Data flow diagrams
- Network diagrams showing firewall or other boundary protection devices segmenting DMZ and internal security zones
- Zero trust architecture, if applicable
- Evidence of lifecycle and configuration management for boundary protection devices
- Network architecture

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
✓	✓	✓	✓

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

- Network perimeter security policy, standard, and procedures
- Internal corporate network security policy, standard, and procedures
- Network management policy, standard, and procedures
- Mobile device security standard
- Related framework and strategy documents
- Network device baseline configuration documents
- Network architecture

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
✓	✓	✓	✓

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

- Computer system access control policy
- Network security standard
- Remote connectivity security policy, standard, and procedures
- Authentication security policy, standard, and procedures
- Secure remote working awareness materials
- Documented rationales for the risk-based decisions regarding the use or non-use of MFA
- Various system security documentation
- User access review (VPN, PIN logon, etc.)
- Remote access and/or telecommuting security policy and procedures

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
✓	✓	✓	

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

- Database security standard
- Network details and diagrams
- Network security standards
- Server inventory and standards
- Web technologies security standard
- Software development lifecycle documentation
- Developer and administrator access controls
- Production data change management procedures

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
✓	✓	✓	

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

- Network device baseline configuration documents
- Controls implemented for secure configurations
- Related network device configuration policies, standards, and procedures
- Procedures relating to the use of centralized configuration management tools
- Inventory of operational technology systems

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
✓	✓	✓	✓

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

- Related policies and procedures
- End-user agreements
- BYOD policies
- Related employee training
- Data encryption
- Technical controls to address risks of personal devices accessing the organization's network and resources

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
✓	✓	✓	✓

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.

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

- Documentation of environmental and physical controls
- Business continuity/resiliency plans
- Data backup and recovery policy, standard, and process
- Backup and restore standards and plans, inclusive of critical applications
- Backup and restore testing standards and process
- Formal backup and recovery testing documentation
- Documentation evidencing annual tests of systems, applications, and data recovery
- Resilience strategy and framework
- Technology Architecture

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
✓	✓		

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

- Data center recovery strategy and procedures
- Asset risk assessment criteria and evaluation process
- Business continuity, resiliency, incident management, and disaster recovery plans
- Third-party policies, standards, and procedures
- Evidence that critical online systems and processes are tested to withstand stresses for extended periods (e.g., DDoS)
- Evidence of testing the ability to shift business processes or functions between different processing centers or technology systems for cyber incidents without interruption to business or loss of productivity or data
- Resilience strategy
- Technology architecture

CYBER RISK INSTITUTE

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
✓	✓		

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 operational and network monitoring intersect with event detection, incident identification, and incident management processes.

Examples of Effective Evidence

- Inventory of network resources and network connections
- Related baseline measures
- Related network diagrams and reporting showing connectivity and data flows
- Related assessments
- Related processes and procedures
- Verification that network and system diagrams are stored in a secure manner with proper restrictions on access
- Validation of an accurate asset inventory
- Incident management procedures
- Capacity planning analyses and estimates

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
✓	✓	✓	

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

- Capacity management policy
- Service level management standard
- Service review process documentation
- Inventory system
- Operations reporting
- Related risk and control assessments

DETECT

Continuous Monitoring (DE.CM)

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
✓	✓	✓	✓

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

- Intrusion detection policy and procedures
- Insider threat policy and procedures
- Intrusion detection alert metrics (e.g., number of alerts, types of alerts, monthly or quarterly reports,)
- Process description
- Proof of analyzing potential unusual activity
- Proof that mechanisms or tools are in place to alert management to potential attacks (e.g., antivirus alerts, log event alerts) and trigger the incident response plan
- Proof of related reporting

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
✓	✓	✓	

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

- Monitoring/detection policies and procedures
- Process description
- Proof of monitoring of potential attacks
- Proof that mechanisms and tools are in place to alert management to potential attacks (e.g., antivirus alerts, log event alerts)
- Proof that a risk-based solution is in place at the institution or Internet hosting provider to mitigate disruptive cyber-attacks (e.g., DoS/DDoS attacks)
- Proof of related reporting

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
✓	✓	✓	

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.

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

- Network security policies, standards, and procedures
- Remote connectivity security policies, standards, and procedures
- Business systems security policies, standards, and procedures based on applications that provide integrated data, video, and voice in one supported product
- Network management policies, standards, and procedures
- Internet connection policies, standards, and procedures
- Allow or deny lists
- Proof that mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks
- Proof that processes are in place to monitor for the presence of unauthorized users, devices, connections, and software
- Documents on related tools for preventing, monitoring, and remediating unauthorized access from/to devices, connections and data transfers are in place
- Proof that role-based access reviews are effective and timely
- Related reporting

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Related tools
- Related reporting
- Applications and supporting infrastructure security testing policies, standards, and procedures
- Vulnerability management security policies, standards, and procedures
- Proof that vulnerability scans are utilized to provide insight into the effectiveness of the patch management process

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
✓	✓	✓	✓

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

- Blocking process description
- Allow or deny lists
- Proof that related tools for preventing, monitoring, and remediating inappropriate or malicious websites are in place
- Related reporting
- Proof of email protection mechanisms that filter for common cyber threats (e.g., attached malware or malicious links)

CYBER RISK INSTITUTE

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
✓			

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 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

- Deception techniques and technologies
- Intrusion detection policy and procedures
- Insider threat policy and procedures
- Intrusion detection alert metrics (e.g., number of alerts, types of alerts, monthly or quarterly reports, etc.)
- Process description
- Proof of analyzing potential unusual activity
- Proof that mechanisms or tools are in place to alert management to potential attacks (e.g., antivirus alerts, log event alerts) and trigger the incident response plan
- Proof of related reporting

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
✓	✓	✓	✓

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

- Event logging and monitoring/detection policies, procedures, standards, and processes
- Proof of monitoring and logging to detect anomalous activities and potential cybersecurity events
- Related tools
- Related reporting
- Proof that physical security controls used to prevent unauthorized access to information systems and telecommunications systems are in place and operating effectively

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
✓	✓	✓	✓

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

- Access request and review security policies, standards, and procedures
- Security event logging and monitoring policies, standards, and processes
- Related logging and monitoring reports
- Proof of monitoring to detect anomalous activities across the environment

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
✓	✓	✓	✓

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

- Event logging and monitoring policy, standard, and process
- Description of controls
- Use cases
- Proof of related reporting
- Proof that mechanisms and tools are in place to alert management of potential misuse (e.g., antivirus alerts, log event alerts)
- Proof that roll-based monitoring of access to critical systems by third parties for unauthorized or unusual activity occurs
- Proof of monitoring users with elevated privileges
- Proof that processes are in place to monitor for the presence of unauthorized users, devices, connections, and software
- Insider threat program

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
✓	✓	✓	

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

- Event logging and monitoring policy, standard, and process
- Proof that anomalous activities can be detected by monitoring elevated privileges across the environment
- List of privileged users
- Use cases
- Proof that mechanisms and tools are in place to alert management to potential misuse by users with elevated privileges and trigger the incident response plan (e.g., antivirus alerts, log event alerts)
- Related reporting

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
✓	✓	✓	✓

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

- Third-party policies, standards, and processes
- Third-party contracts and other approvals (e.g., Board meeting minutes)
- Inventory of third-parties and any related reporting
- Risk assessment programs/processes
- Network diagrams identifying all external connections to third-parties
- Use cases
- List of related tools for monitoring third parties to detect potential cybersecurity events
- Connections, data transfer, API design documentation

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
✓	✓	✓	

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

- Access request and review security policies, standards, and procedures
- Security event logging and monitoring policies, standards, and processes
- Contracts with third-party service providers
- Risk assessment program/process
- Related logging and monitoring reports
- Proof of monitoring to detect anomalous activities across the environment
- Related tools and reporting for monitoring third parties to detect potential cybersecurity events

CYBER RISK INSTITUTE

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
✓	✓		

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

- Endpoints security policy, standard, process
- File integrity monitoring processes and procedures
- Anti-malware security standard
- System Development Life Cycle (SDLC) Policy, standards, and procedures
- Third-party processes and procedures
- System hardening guidelines
- Mobile device management processes and procedures

DE.CM-09.02: The organization uses integrity checking mechanisms to verify hardware integrity.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

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

- Hardware, BIOS, and operating system monitoring documentation
- Integrity checking mechanisms

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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

- Unsupported and unauthorized software, hardware, configuration change identification/review process and reports
- Configuration management policies, standards, and processes
- Software management policies, standards, and processes
- Hardware management policies, standards, and procedures
- Proof that related tools for preventing, monitoring, and remediating of unauthorized software, hardware, configuration are in place
- Supported software, hardware, configuration changes
- Documentation that programs that can override system, object, network, virtual machine and application controls are restricted

Adverse Event Analysis (DE.AE)

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:

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

(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.

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.

Examples of Effective Evidence

- Security logging and monitoring policies, standards, and procedures
- Security incident response policies and procedures
- Documents on mechanisms or tools in place (e.g., antivirus alerts, documentation of configuration settings, custom detection methods, event logs)
- Documents that show detection metrics are analyzed to understand attack targets and methods
- Related reporting
- Risk assessments to predict threats and drive real-time responses
- Profiles for each threat that identifies the likely intent, capability, and target of the threat
- Cyber threat summaries that utilize threat intelligence to identify the institutions risk and actions to be taken in response

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
✓	✓	✓	✓

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 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

- Security information and event management (SIEM) documentation
- Documents on methods in place for monitoring across the environment to detect anomalous activities
- Documents on mechanisms or tools in place to alert management (e.g., detection methods and searches, automated playbooks, etc.)
- Documents showing that incident alert parameters and thresholds are established
- Examples of third-party alert procedures/agreements with critical service providers
- Related reporting
- Documents showing that alert parameters are set for detecting information security incidents that prompt mitigating actions
- System performance reports contain information that can be used as a risk indicator to detect information security incidents

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
✓	✓	✓	✓

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

- Event logging, monitoring, detecting, and alerting methodology
- Examples of event logging
- Documentation of the monitoring of logs and ports
- Documents on mechanisms and tools in place to alert management to potential attacks (e.g., antivirus alerts, log event alerts) and trigger the incident response program
- Related reporting
- Documents showing the physical environment is monitored to detect potential unauthorized access
- System performance reports containing information that can be used as a risk indicator to detect an information security incident

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
✓	✓	✓	✓

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

- Documents on tools and processes in place to detect, alert, and trigger the incident response program (e.g., cyber threat intelligence sources and aggregators, log repository and correlation, etc.)
- Use cases to document how alerts will be handled (e.g., playbooks, custom detection methods, etc.)
- Data sources confirming both internal and external coverage
- Log reporting examples showing how the institution detects anomalous activities through monitoring activity across the environment
- Policies and procedures explaining how threat information is used to monitor threats and vulnerabilities
- Documents showing that the review of correlation events aligns with the organization's cybersecurity response/standards

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
✓	✓	✓	✓

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.[14]

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

- Risk policies, standards, and procedures
- Security incident response plan
- Crisis management plan, including impact risk assessment and communication
- Process description and flows
- Event management framework
- Related reporting
- Identification of root cause(s) and impact when cyber attacks result in material loss
- Quantification methodologies to determine materiality

[14] 17 CFR Parts 229 and 249, Securities and Exchange Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Disclosure Obligations Generally.

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
✓	✓	✓	✓

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

- Security incident response policies, standards, and procedures addressing the concepts of threat information sharing
- Related policies, standards, and procedures for reacting and responding to cyber incidents
- Cybersecurity incident response plan example
- Event/incident escalation procedures and triage process
- Proof of threat intelligence collection, correlation, and dissemination process and reporting
- Related reporting and alert examples
- Use cases
- Board or board subcommittee meeting minutes showing newsworthy cyber events or regulatory alerts are addressed.
- Information security threats and materials gathered and shared with applicable employees
- Proof of threat information shared with law enforcement and regulators

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
✓	✓		

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

- Products, reports, notifications, or dashboards on cyber threat intelligence (e.g., threat intelligence dashboard)
- Cyber threat intelligence and threat analysis reports
- Subscription to threat intelligence feeds that inform the organization of changing threat condition over time
- Cyber threat intelligence policies and standards
- Cyber threat intelligence reporting

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
✓	✓	✓	

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

- Security event logging and monitoring policy, standard, and procedure
- Examples of tools used
- Related procedure documents
- Event detection and correlation metrics (monthly, quarterly, or annually) are analyzed to understand attack targets and methods
- Incident response metrics and examples
- Related reporting and escalations
- Event report templates

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
✓	✓	✓	

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

- Security incident response policies, standards, and procedures
- Cybersecurity incident response plan example
- Playbooks or other incident response related plans and processes
- Impact assessments
- Documented severity levels
- Third-party security policy, standard, and procedures
- Contract with third parties, including no delegation clause or equivalent

RESPOND

Incident Management (RS.MA)

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
✓	✓	✓	✓

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

- Security incident response policies, standards, and procedures
- Cybersecurity incident response plan example
- Playbooks or other incident response related plans and processes

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
✓	✓	✓	✓

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

- Security incident response policies, standards, and procedures
- Incident response examples or playbooks
- Security logging and monitoring policy, standard, and procedure
- Related security logging and monitoring tools
- Logging and Monitoring use cases
- Alerting use cases and thresholds
- Logging and reporting examples
- Related assessment reporting

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Security incident response policies, standards, and procedures
- Incident response examples or playbooks
- Event/incident escalation and prioritization procedures

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
✓	✓	✓	

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.

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

- Security incident response policies, standards, and procedures
- Documented tracking response progress and milestones
- Incident response examples or playbooks
- Event/incident system of record
- Related documentation and examples

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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

- Security incident response policies, standards, procedures
- Security incident reporting templates which support a consistent, repeatable process
- Incident response examples or playbooks
- Related documentation and examples
- Related training material

Incident Analysis (RS.AN)

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
✓	✓	✓	✓

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

- Security incident response policies, standards, and procedures
- Security logging and monitoring policy, standard, and procedure
- Roles and responsibilities (i.e., forensics, root cause analysis teams)
- Contracts or retainer agreements for forensic investigation expertise
- Use cases
- Related assessment reporting

CYBER RISK INSTITUTE

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
✓	✓	✓	

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

- Forensic security policies, standards, and procedures
- Forensic playbooks or other use case where forensics was conducted on a live incident
- Evidence of appropriate skills (i.e., certification) and training in forensics for those in the role

CYBER RISK INSTITUTE

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
✓	✓	✓	

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

- Security incident response policies, standards, and procedures
- Security logging and monitoring policy, standard, and procedure
- Roles and responsibilities (i.e., forensics, root cause analysis teams)
- Contracts or retainer agreements for forensic investigation expertise
- Use cases
- Related assessment reporting

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 not the incident constitutes a material event.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

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.[15]

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

- Risk policies, standards, and procedures
- Security incident response plan
- Crisis management plan, including impact risk assessment and communication
- Process description and flows
- Event management framework
- Related reporting
- Identification of root cause(s) and impact when cyber attacks result in material loss
- Quantification methodologies to determine materiality

[15] 17 CFR Parts 229 and 249, Securities and Exchange Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Disclosure Obligations Generally.

Incident Response Reporting and Communication (RS.CO)

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.

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 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

- Security incident response policies, standards, and procedures
- Incident response examples or playbooks
- Related notification procedures
- Related documentation and examples
- Information classification and handling guidelines

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
✓	✓	✓	✓

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

- Security incident response policies, standards, and procedures
- Incident response examples or playbooks
- Related notification procedures
- Related documentation and examples

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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

- Security incident response policies, standards, and procedures
- Incident response examples or playbooks
- Incident response process, major incident management process, or other related notification procedures
- Cyber threat/incident information sharing examples
- Related testing of incident response communications
- Communication plan activities
- Automated notification tools in use

CYBER RISK INSTITUTE

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
✓	✓	✓	

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

- Cyber threat intelligence sharing policies, procedures, or standards
- Cyber threat intelligence reporting examples
- Roles and responsibilities of cybersecurity and business unit staff

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
✓	✓	✓	✓

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

- Security incident response policies, standards, and procedures
- Incident response examples or playbooks
- Related notification procedures
- Cyber threat/incident reporting examples
- Regulators and law enforcement notification and reporting requirements

Mitigation (RS.MI)

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
✓	✓	✓	✓

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

- Vulnerability management security standard
- Remediation management documentation
- Related examples
- Related reporting

TIER 1	TIER 2	TIER 3	TIER 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.

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

- Vulnerability management security standard
- Incident response policies, standards, and plans
- Remediation management documentation
- Related examples
- Related reporting

RECOVER

Recovery Planning (RC.RP)

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
✓	✓	✓	✓

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

- Security incident response policy, standard, procedures
- Incident response examples or playbooks
- Business continuity/resilience policy, standard, and procedures
- Data backup and recovery policy, standard, and procedures
- Disaster recovery plans

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
✓	✓	✓	✓

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

- Security incident response policies, standards, procedures
- Incident response examples or playbooks
- Related documentation and examples
- Related task plans, response activities
- Related prioritization
- Roles and responsibilities for response plans

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
✓	✓	✓	✓

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

- Business continuity/resilience policy, standard, and procedures
- Data center recovery procedures
- Business recovery procedures
- Other related recovery procedures

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
✓	✓	✓	✓

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

- Business continuity/resilience policy, standard, and procedures
- Verification of recovery capabilities
- Related restoration steps
- Data center recovery procedures
- Business recovery procedures
- Other related recovery procedures

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
✓	✓	✓	✓

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

- Business continuity/resilience policy, standard, and procedures
- Verification of recovery capabilities
- Related restoration steps
- Data center recovery procedures
- Business recovery procedures
- Other related recovery procedures

CYBER RISK INSTITUTE

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
✓	✓		

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

- Business continuity/resilience policy, standard, and procedures
- Data center recovery procedures
- Business recovery procedures
- Service continuity planning standards and procedures
- Recovery time objectives for critical systems
- Other related recovery procedures

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
✓	✓	✓	✓

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

- Business continuity/resilience policy, standard, and procedures
- Data center recovery procedures
- Business recovery procedures
- Service continuity planning standards and procedures
- Recovery time objectives for critical systems
- Other related recovery procedures

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Business continuity/resilience policy, standard, and procedures
- Post-incident analysis
- Documentation of process improvements
- Relevant meeting notes
- Data center recovery procedures
- Business recovery procedures
- Service continuity planning standards and procedures
- Recovery time objectives for critical systems
- Other related recovery procedures

Communications (RC.CO)

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
✓	✓	✓	✓

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 committees), senior management, incident management support teams, and relevant internal stakeholders.

Examples of Effective Evidence

- Security incident response policy, standard, and procedures
- Business continuity/resilience policy, standard, and procedures
- Incident response examples or playbooks
- Risk governance framework documentation
- Related committee meeting agendas and minutes

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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

- Security incident response policy, standard, and procedures
- Business continuity/resilience policy, standard, and procedures
- Incident response examples or playbooks
- Regulator notification procedure
- Crisis response plan and procedure
- Related reporting and examples

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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

- Security incident response policy, standard, and procedures
- Incident response examples or playbooks
- External communication plan, including media relations
- Business continuity/resilience policy, standard, and procedures
- Regulator notification procedure
- Crisis response plan and procedure
- Related reporting and examples

Procurement Planning and Due Diligence (EX.DD)

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
✓	✓	✓	

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract with third parties
- Risk assessments
- Procurement plans
- Third-party risk management governance roles and responsibilities
- Due diligence policy, requirement, or questionnaire
- Other related third-party assessment processes, examples, and reporting

CYBER RISK INSTITUTE

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
✓	✓		

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.

Examples of Effective Evidence

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract with third parties
- Procurement plans
- Risk assessments
- Inherent risk analysis documentation
- Third-party risk management governance roles and responsibilities
- Due diligence policy, requirement, or questionnaire
- Other related third-party assessment processes, examples, and reporting

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
✓	✓		

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract with third parties
- Procurement plans
- Risk assessments
- Third-party risk management governance roles and responsibilities
- Due diligence policy, requirement, or questionnaire
- Other related third-party assessment processes, examples, and reporting

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
✓	✓	✓	✓

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 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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract with third parties
- Procurement plans
- Risk assessments
- Third-party risk management governance roles and responsibilities
- Due diligence policy, requirement, or questionnaire
- Other related third-party assessment processes, examples, and reporting

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
✓	✓	✓	✓

Response Guidance

Procurement due diligence 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, costs imposed on the organization, and any incentives and/or penalties 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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract with third parties
- Procurement plans
- Risk assessments
- Third-party risk management governance roles and responsibilities
- Due diligence policy, requirement, or questionnaire
- Other related third-party assessment processes, examples, and reporting

TIER 1	TIER 2	TIER 3	TIER 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 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.

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Documented processes to review and evaluate documentation of a prospective critical third party
- Contract with third parties
- Procurement plans
- Risk assessments
- Third-party risk management governance roles and responsibilities
- Due diligence policy, requirement, or questionnaire
- Other related third-party assessment processes, examples, and reporting

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
✓	✓	✓	✓

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract with third parties, including no delegation clause or equivalent
- Risk assessments that third parties have conducted of subcontractors
- Related third-party reporting

EX.DD-03.01: The organization reviews, evaluates, and risk assesses a prospective critical third party's cybersecurity program, including its ability to identity, 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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract with third parties, including no delegation clause or equivalent
- Risk assessments that third parties have conducted of subcontractors
- Related third-party reporting
- Third-party risk management governance roles and responsibilities
- Due diligence policy, requirement, or questionnaire
- Other related third-party assessment processes, examples, and reporting
- Third party due diligence questionnaires

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Inventory of critical external dependencies and business functions
- Identification criteria of critical external dependencies and related business functions
- Third-party security policy, standard, and procedures
- Third-party risk management program
- Critical third-party reporting or other related reporting
- Contract reporting
- Third-party risk management governance roles and responsibilities
- Due diligence policy, requirement, or questionnaire
- Other related third-party assessment processes, examples, and reporting

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
✓	✓	✓	✓

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract with third parties, including no delegation clause or equivalent
- Risk assessments that third parties have conducted of subcontractors
- Related third-party reporting
- Third-party risk management governance roles and responsibilities
- Due diligence policy, requirement, or questionnaire
- Other related third-party assessment processes, examples, and reporting

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
✓	✓		

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

- Application security testing policy, standards, and procedures
- Security testing policy, standards, and procedures for applications in use, including externally developed applications
- Related application testing evidence

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
✓	✓	✓	✓

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract with third parties, including no delegation clause or equivalent
- Risk assessments that third parties have conducted of subcontractors
- Related third-party reporting
- Third-party risk management governance roles and responsibilities
- Due diligence policy, requirement, or questionnaire
- Other related third-party assessment processes, examples, and reporting

Third Party Contracts and Agreements (EX.CN)

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.

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

- Contract guidance
- Contract clauses
- Contract reporting
- Template/standard contract clauses and terms
- Procurement and contracting policies and procedures

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract guidance
- Contractual language on security requirements (security schedule)
- Contract clauses
- Contract compliance reporting
- Monitoring plans
- Related third-party reporting

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
✓	✓	✓	✓

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract guidance
- Contractual language on security requirements (security schedule)
- Contract clauses
- Contract compliance reporting
- Monitoring plans
- Related third-party reporting

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract guidance
- Contractual language on security requirements (security schedule)
- Contract clauses
- Contract compliance reporting
- Monitoring plans
- Related third-party reporting

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Third-party cybersecurity requirements and related controls
- Contractual language on security requirements (security schedule)
- RFPs or RFIs documenting minimum cybersecurity requirements
- Related third-party reporting

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
✓	✓	✓	✓

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 capability.

Examples of Effective Evidence

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Third-party cybersecurity requirements and related controls
- Contractual language on security requirements (security schedule)
- Examples of contracts with third parties
- Related testing of business continuity program and disaster recovery capability

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Third-party cybersecurity requirements and related controls
- Contractual language on security requirements (security schedule)
- Examples of contracts with third parties
- Related exercises and test
- Related testing results and reports
- Incident response plan
- Documentation evidencing annual tests of systems, applications, and data recovery

Monitoring and Managing Suppliers (EX.MM)

TIER 1	TIER 2	TIER 3	TIER 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 of the third party's products, services, and/or relationship to the organization.

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 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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract guidance
- Contract reporting
- Monitoring processes and reporting
- Related third-party reporting

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
✓	✓		

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract guidance
- Contract reporting
- Monitoring processes and reporting
- Related third-party reporting

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
✓	✓	✓	✓

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract guidance
- Contract reporting
- Continuous monitoring reports
- Monitoring processes and reporting

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
✓	✓	✓	✓

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.

Examples of Effective Evidence

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contractual language on security requirements (security schedule)
- Examples of contracts with third parties

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
✓	✓	✓	

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract guidance
- Contractual language on security requirements (security schedule)
- Contract clauses, including audit rights
- Contract reporting
- Monitoring plans
- Related third-party reporting
- Risk assessments that third parties have conducted of subcontractors

CYBER RISK INSTITUTE

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
✓	✓	✓	✓

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Related risk assessments
- Contract guidance
- Contract clauses, including audit rights
- Contract reporting
- Monitoring plans
- Related third-party reporting

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
✓	✓	✓	✓

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Critical third-party identification procedures
- Critical third-party reporting
- Audit reports
- Contracts clauses, including audit rights
- Related third-party reporting
- Security monitoring reports

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
✓	✓	✓	

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 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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contract guidance
- Contract reporting
- Related third-party reporting

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
✓	✓	✓	✓

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

- Third-party policies, standards, and processes
- Perimeter security policy, standard, and process
- Inventory of third-parties and any related reporting
- Risk assessment program/process
- Use cases
- Related tools for monitoring third-parties to detect potential cybersecurity events

Relationship Termination (EX.TR)

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
✓	✓		

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Exit clauses
- Contingency plans
- Related reporting and examples

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
✓	✓		

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

- Service continuity planning
- Risk reporting
- Test plans
- Examples of Requests for Information (RFI) and Requests for Proposals (RFP)
- Evidence that testing occurred
- Contract clauses

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
✓	✓		

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contractual termination clauses
- Related reporting and examples

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
✓	✓	✓	✓

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Contractual exit clauses
- Related reporting and examples

CYBER RISK INSTITUTE

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
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

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,[16] the FFIEC IT Examination Handbook,[17] the Financial Stability Board (FSB) Cyber Lexicon,[18] and other regulatory sources and international standards. Several terms below are sourced directly from the Profile Glossary,[19] 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 effective strategy for mission assurance, business assurance, or operational resilience.	NIST The MITRE Corporation[20]

[17] Refer to the FFIEC IT Examination Handbooks on the FFIEC website.

[18] Refer to the Financial Stability Board Cyber Lexicon on the FSB website.

[19] Refer to and download the Profile on the CRI website.

[20] Refer to MITRE's Cyber Resiliency Design Principles on MITRE's website.

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	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	NIST
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 space, the perception of an enterprise's security posture and its threat environment	FSB Cyber Lexicon NIST
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

CYBER RISK INSTITUTE

APPENDIX C – FULL DIAGNOSTIC STATEMENTS & IMPACT TIER

	DIAGNOSTIC STATEMENT	IMPACT TIER
	GOVERNANCE	
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
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 4) Incorporating the potential impact of an incident into their BCM process and ensure resilience capabilities are in place.	1 2 3 4
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, geographical/geopolitical exposure, fourth-party impacts, and financial sector co-dependencies.	1	2		
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
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
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 organization adapts to the evolving risk environment while remaining within its stated risk appetite and tolerance.	1	2	3	4
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	
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
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);	1 2 3 4

	(2) Vulnerability sharing forums (e.g., FS-ISAC); and (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 resourc (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 ar involved in testing as part of a crisis management team and are informed of test results.	1	2		
ID.IM-02.08	The organization tests and exercises, independently and in coordination with other critical sector partnei 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.	1			
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 and improv 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 ir 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 an 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 an 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 it 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 granting acces 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
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, credenti 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 separatior of duties (e.g., through role-based access control, asset owner access recertifications, 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 othe systems) lifecycles to ensure strict security over creation, use, and termination; access credentials (e.g.,	1	2	3	4

	no embedded passwords in code); frequent reviews of account ownership; visibility for unauthorized use and hardening against malicious insider use.		
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/roo 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, all impacte personnel (e.g., end-users, developers, operators, etc.) are trained on the new system and any accompanying technology and cybersecurity risks.	1	2 3 4
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.	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 operationa 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 perform 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 th 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 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.	1	2 3 4
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).	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 media (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 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).	1	2 3 4

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.	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 performir backup restoration testing.	1	2	3	4
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 setting configurations, and versions.	1	2	3	
PR.PS-01.02	The organization's systems are configured to provide only essential capabilities to implement the princip 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 rectified.	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 practice 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 peripheral 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 patcl criticality and risk, test patches, and apply patches within risk/criticality-based target time frames.	1	2	3	4
PR.PS-02.02	The organization establishes standards and practices for ongoing application management to ensure tha applications remain secure and continue to meet organizational needs.	1	2		
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.	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, to 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 control 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
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 use 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.) during 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 services 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 and 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 documented, 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 stated requirements, SLAs, or OLAs) and performance is monitored and regularly reported to stakeholders.	1	2			
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 networks proce by implementing appropriate mechanisms (e.g., strong authentication for authentication and transmissio 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 netwo 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 normal 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 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 volumes 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		
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 and 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 potential intrusion events across the organization's physical environment and infrastructure, including the detectic of environmental threats (fire, water, service outages, etc.) and unauthorized physical access to high-ris 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 an 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 monitoring 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 service 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 the 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;	1	2	3	4	

	(2) Predict and block a similar future attack; and (3) Report timely risk metrics.					
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 perimeter 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	
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 for efficie 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 and 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, conductir investigations, and collecting and preserving evidence per best practices and forensic 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 not 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, linke 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 required, government bodies, self-regulatory agencies and/or other supervisory bodies, within required timeframes	1	2	3	4	

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, to authorized staff with responsibility for the mitigation of cyber risks at the strategic, tactical and operationa 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 its 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-par 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 busine 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 adapted 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 entities 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 other 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, an 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 ha 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 authorities 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 abo an incident.	1	2 3 4

SUPPLY CHAIN / DEPENDENCY MANAGEMENT

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.	1	2 3
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.	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 knowledg and experience, to conduct third party due diligence consistent with the procurement 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 fe 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.	1	2 3 4
EX.DD-02.03	The organization reviews and evaluates documentation, such as financial statements, independent audi 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.	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 deliverir 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 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.	1	2 3 4
EX.DD-03.02	The organization reviews and evaluates a prospective critical third party's business continuity program, t include business impact analyses, risk assessments, continuity plans, disaster recovery plans, technolo 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 incluc 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.	1	2 3 4
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 to 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 to regularly participate in joint and/or bilateral recovery exercises and tests, and to address significant issu identified through recovery testing.	1	2	3	4
EX.MM-01.01	The organization implements procedures, and allocates sufficient resources with the requisite knowledg and experience, to manage and monitor its third-party relationships to a degree and extent commensura 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.	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 risk 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 own supplie and partners (fourth and nth parties) and the risks those fourth and nth parties may pose to the third par and to the organization (e.g., cybersecurity supply chain risk, concentration 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 critical fourth parties, to confirm contract controls are maintained and compliance requirements are managed.	1	2	3	4
EX.MM-02.01	The organization conducts regular third-party reviews for critical vendors to validate that requisite securit 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 in 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 products, services, and external connections.	1	2	3	4
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.	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 addressed in a timely manner.	1	2	3	4