CYBER RISK INSTITUTE

The Profile Workbook

Guidance for Implementing the CRI Profile v1.2 and Responding to its Diagnostic Statements

Last updated: December 2021

Cyber Risk Institute

Washington, DC

cyberriskinstitute.org

CYBER RISK INSTITUTE

We would like to thank Ann Lavis, Heidi Erchinger, and Kevin Isabelle from HSBC who developed the first comprehensive draft of the Profile Workbook. Their work is of tremendous benefit to the Profile and the industry overall.

We would also like to thank Stephanie Wake of the Bank Policy Institute-BITS and Kevin Gronberg of CRI. Their leadership of the review process, as well as their substantive contributions were essential for this document's development, finalization, and release.

-The CRI Team

CYBER RISK INSTITUTE

TABLE OF CONTENTS

CYBER RISK INSTITUTE

ABOUT THE PROFILE WORKBOOK

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 277 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 Workbook* is to (1) assist organizations in implementing the Profile and (2) drive consistency when completing the Profile within the financial sector. The *Profile Workbook* provides interpretive guidance on each of the CRI Profile's 277 Diagnostic Statements and examples of effective evidence to support the organization's response.

The *Profile Workbook* 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 Workbook* 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

---

[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.

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 program can use and leverage the *Profile Workbook* to implement the Profile, including information security risk, cybersecurity, legal, audit and prudential regulator examination staff.

Contents

This *Profile Workbook* is intended to provide guidance for responding to all 277 Diagnostic Statements, outlined by Function and Category. Users can navigate to each of the 277 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 included for each Diagnostic Statement are not meant to be exclusive or exhaustive, but merely guidance on 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 listed within the *Profile Workbook*. Further, these examples 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.

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 277 Diagnostic Statements

Tier 2: Subnational Impact includes 262 Diagnostic Statements

Tier 3: Sector Impact includes 188 Diagnostic Statements

Tier 4: Localized Impact includes 137 Diagnostic Statements

Response Key

Organizations note the outcome of their assessment by selecting between eight potential Diagnostic Statement responses:

1) **Yes:** An institution would select this response if it can confidently answer that it fulfills this Diagnostic Statement;
2) **No:** An institution would select this response if it has not fulfilled the Diagnostic Statement;
3) **Partial:** An institution would select this response if it has not fully met the Diagnostic Statement, but is currently working through an action plan to achieve a "Yes" outcome;
4) **Not Applicable:** An institution might select this response if, after evaluating its business and security program, the Diagnostic Statement is not applicable even though it was suggested by its Impact Tier;
5) **Not Tested:** An institution might select this response if it has yet to test controls associated with that particular Diagnostic Statement;
6) **Yes-Risk Based:** An institution might select this response if the Diagnostic Statement, in referring to supervisory language, requires a more nuanced, risk-based answer and explanation than the Diagnostic Statement otherwise suggests;
7) **Yes-Compensating Controls Used:** An institution might select this response if it meets the intent of the Diagnostic Statement by using compensating controls; and
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 Workbook* 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 Workbook*:

- 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

GOVERNANCE

Strategy and Framework (GV.SF)

GV.SF-1.1: The organization has a cyber risk management strategy and framework that is approved by the appropriate 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 cyber risk management strategy and framework should be a prominent part of all business strategies, practices, policies, and procedures. The cyber risk management strategy 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 cyber risk management strategy and framework. Document the approval of the strategy and framework by the Board (or one of its committees) and outline how the strategy/framework incorporates business strategy and links to the enterprise risk management framework. For example, the cyber risk management framework may be part of the organization's overall enterprise risk management framework. Describe how that framework is established and executed for cyber risk management.

Examples of Effective Evidence

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

CYBER RISK INSTITUTE

GV.SF-1.2: An appropriate governing authority (e.g., the Board or one of its committees) oversees and holds senior management accountable for implementing the organization's cyber risk management strategy and framework.

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 cyber risk management program and should ensure compliance with 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 cyber risk management strategy and framework. 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 cyber risk management strategy and framework (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 cyber risk management strategy and framework. Provide organizational charts to identify responsible/accountable executives.

Examples of Effective Evidence

- Cyber risk management strategy and framework, including evidence of approval by appropriate governing authority
- Policies, standards, controls, procedures, and guidelines specific to cyber 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 cyber 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 cyber risk management
- Senior management scorecards on operating effectiveness, including key performance indicators (KPIs) and key risk indicators (KRIs)

GV.SF-1.3: The organization's cyber risk management strategy identifies and documents the organization's role as it relates to other critical infrastructures outside of the financial services sector and the risk that the organization may pose to them.

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[6] and critical functions set[7] are used to identify relevant sectors. In the United Kingdom the Centre for the Protection of National Infrastructure defines critical national infrastructure.[8] The Board or Committee should be aware of any critical infrastructure that the organization's services or activities could impact due to a cyber breach. 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. Cybersecurity strategies should recognize the organization's role with respect to critical infrastructure functions. Include details on how the cyber risk management strategy is related to other critical infrastructures outside of the financial sector (e.g., energy, communications, information technology, etc.).

Examples of Effective Evidence

- Cyber risk management strategy 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)

[6] www.cisa.gov/critical-infrastructure-sectors
[7] www.cisa.gov/national-critical-functions-set
[8] https://www.cpni.gov.uk/critical-national-infrastructure-0

CYBER RISK INSTITUTE

GV.SF-1.4: The cyber risk management strategy identifies and communicates the organization's role within the financial services sector as a component of critical infrastructure in the financial services industry.

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[9] and the UK's Centre for Protection of National Infrastructure (CPNI)[10]. 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.[11]

Responses should include how the cyber risk management strategy has both identified and communicated the organization's role within the sector as a component of critical infrastructures 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)[12] or similar organization to address critical sector impacts.

Examples of Effective Evidence

- Cyber 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)
- Attestation documentation 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)
- Cyber dashboards demonstrating controls effectiveness

---

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

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

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

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

GV.SF-1.5: The cyber risk management strategy and framework establishes and communicates priorities for organizational mission, objectives, and activities.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

Describe how the cyber risk management strategy and framework establishes priorities for organizational mission, objectives, and activities and communicates those priorities. Response should include documentation, such as the target operating model (i.e., desired state of operations considering the organization's role in critical infrastructure) and related documents supporting the cyber risk management strategy and framework and the establishment and communication of priorities for the organizational mission, objectives, and activities.

Examples of Effective Evidence

- Organizational mission statement
- Cyber risk management 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)
- Mission statement
- Organizational charts
- Roles and responsibilities

GV.SF-2.1: The cyber risk management strategy and framework is appropriately 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 apply industry security standards and guidelines when it analyzes cybersecurity risk and gaps in controls and processes. Responses should include evidence that the cyber risk strategy and framework are built upon these industry standards and guidelines. Additionally, responses should provide evidence of cyber risk strategy and framework initiatives and projects that are aligned to, or implemented in accordance with, 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 resource sufficient for this purpose.

Examples of Effective Evidence

- Cyber risk management strategy and framework, including evidence of consistency with 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.SF-3.1: An appropriate governing authority (e.g., the Board or one of its committees) endorses and periodically reviews the cyber risk appetite and is regularly informed about the status of and material changes in the organization's inherent cyber 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 define certain risk tolerance metrics that help 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 not in isolation by any one person or department. These statements should be further reviewed and approved, if appropriate, by the Board. Responses should provide information and examples of cyber risk appetite and risk tolerance, including the oversight, review, and approval processes. Include various board and committee information, organizational charts, roles, and responsibilities. For organizations that do not use specific risk appetite statements, describe how the organization's governing authority reviews cyber risk and updates procedures based on cyber threats.

Organizations should demonstrate that there is a defined process to elevate the existence of a cyber risk 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
- Cyber risk escalation process

GV.SF-3.2: An appropriate governing authority (e.g., the Board or one of its committees) periodically reviews and evaluates the organization's ability to manage its cyber risks.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization should have a process evaluating changes to the organization's cyber 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.

Provide information that demonstrates the appropriate governing authority reviews (scope, frequency, etc.) and evaluates the effectiveness with which the organization can manage its cyber 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.SF-3.3: The cyber risk management framework provides mechanisms to determine the adequacy of resources to fulfill cybersecurity objectives.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

Resources, including funding and technical/managerial talent, contribute to the effectiveness of the 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 cybersecurity risks and to determine resources required for mitigating gaps. 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 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 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

GV.SF-4.1: The risk appetite is informed by the organization's role in critical infrastructure.

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, because of 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. If conservative, what aspects contribute to being conservative. 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, key risk indicators (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)
- Corporate risk framework

Risk Management (GV.RM)

GV.RM-1.1: The cyber risk management program incorporates cyber risk identification, measurement, monitoring, and reporting.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization's cyber risk management program should consider the likelihood and impact of cyber 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 cyber risk management program incorporates cyber 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 cyber risk reduction.

Examples of Effective Evidence

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

GV.RM-1.2: The cyber risk management program is integrated into daily operations and is tailored to address enterprise-specific risks (both internal and external) and evaluate the organization's cybersecurity policies, procedures, processes, and controls.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

The consideration of cyber risks should be embedded in strategic and tactical planning activities and not managed as a downstream or separate function. The organization should implement a formal process that ensures cyber risks are considered across business units within the organization.

Describe and provide evidence supporting the cyber risk management program linkage to the operational risk management framework. Provide information on the three lines of defense and the responsibility of each line to evaluate and manage cyber risk. Describe how any 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
- 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-1.3: As a part of the cyber risk management program, the organization has documented its cyber risk assessment process and methodology, which are periodically updated to address changes to the risk profile and risk appetite (e.g., new technologies, products, services, interdependencies, and the evolving threat environment).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

Cybersecurity-related risks should be identified, reviewed, and analyzed as part of the organization's risk assessment processes. New products and services as well as outsourced relationships have the potential of introducing new or expanding existing cybersecurity risks. Such risks should be evaluated to determine whether appropriate controls are in place. In addition, the cyber threat environment is highly dynamic and prominent threats can necessitate revisiting these risk assessments. Risk assessments are not a one-time activity. At least once a year, senior management should review the entire risk assessment to ensure relevant information is appropriately considered. 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 cyber risk assessment process and methodology is documented and updated at least annually. Demonstrate how cybersecurity 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 an information 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-1.4: The cyber risk assessment process is consistent with the organization's policies and procedures and includes criteria for the evaluation and categorization of enterprise-specific cyber risks.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The cyber risk assessment 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 cyber risk assessment 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 cyber risk assessment process is aligned with the organization's policies and procedures. Highlight the criteria used for the evaluation and categorization of enterprise-specific cyber risks, and threats, and vulnerabilities.

Examples of Effective Evidence

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

GV.RM-1.5: The cyber risk management program and risk assessment process produce actionable recommendations that the organization uses to select, design, prioritize, implement, maintain, evaluate, and modify security controls.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Management should have a methodology to measure and document cybersecurity risks and for determining resources required for mitigating gaps. The cyber 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 assess the likelihood and potential damage of these threats, and validate whether policies, procedures, and controls in place are appropriately mitigating risks. 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 cybersecurity recommendations that are prioritized and tracked. Provide evidence of 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

GV.RM-1.6: The cyber risk management program addresses identified cyber risks in one of the following ways: risk acceptance, risk mitigation, risk avoidance, or risk transfer, which includes cyber insurance.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The cyber risk management program should consider the likelihood and impact of cyber 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 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 each.

Examples of Effective Evidence

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

GV.RM-2.1: The organization has established a cyber-risk tolerance consistent with its risk appetite, and integrated it into technology or operational risk management, as appropriate.

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. Provide evidence of linkage between key risk indicators (KRIs) and risk appetite/risk tolerance. Describe the process of defining and updating the risk appetite 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-2.2: The cyber risk management strategy articulates how the organization intends to address its inherent cyber risk (before mitigating controls or other factors are taken into consideration).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

Describe how the cyber risk management strategy articulates the methodology and intention of the organization to address its inherent cyber risk (before mitigating controls or other factors are taken into consideration). Describe the programs in place to address perimeter security, application security, infrastructure protection, etc. Provide information on the cyber risk management framework used.

Examples of Effective Evidence

- Cyber risk management strategy and framework
- 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

GV.RM-2.3: The cyber risk management strategy articulates how the organization would maintain an acceptable level of residual cyber risk set by the appropriate 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 tolerance level and monitor outliers until risks are mitigated. High and moderate residual 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

- Cyber 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 cyber risk
- Specific organization tools/methods for cyber risk quantification
- Control environment and control effectiveness reports

GV.RM-3.1: The cyber risk management framework is integrated into the enterprise risk management framework.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

The cyber risk management framework and threat intelligence analysis process should be integrated with the enterprise risk management process to ensure the risk of relevant threats is analyzed and mitigating controls or alerts can be implemented. Enterprise risk management objectives and actions encompass 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 cyber risk management framework 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

- Cyber risk management strategy and framework
- Enterprise risk management strategy and framework
- Cyber risk assessment methodology
- 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-3.2: The organization has a process for monitoring its cyber risks including escalating those risks that exceed risk tolerance to management.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

When cyber risk that exists within the organization exceeds the maximum acceptable risk tolerance, 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 cyber risk and the appropriate methods and channels to escalate potential cybersecurity issues. Response should include a description of the process for cyber risk monitoring and escalation.

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.)
- Cyber reporting, dashboards, and briefs
- Relevant Board and committee (e.g., Risk committee) meeting agendas and minutes

GV.RM-3.3: The organization's cyber risk management framework provides for segregation of duties between policy development, implementation, and oversight to ensure rigorous review of both policy and implementation.

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 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

Policy (GV.PL)

GV.PL-1.1: The organization maintains a documented cybersecurity policy or policies approved by a designated Cybersecurity Officer (e.g., CISO) or an appropriate governing authority (e.g., the Board or one of its committees).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization should have a cybersecurity policy, standards and procedures that align with risk and complexity maintained by the designated Cybersecurity Officer (e.g., CISO). Generally, the cybersecurity policy 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 policy. The Board or one of its committees is responsible for overseeing the organization's cybersecurity program, including reviewing and approving cybersecurity policies.

Provide information regarding the organizational structure for the management and operation of 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) and updated on a regular basis. Describe how 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

- 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.PL-1.2: The organization's cybersecurity policy integrates with an appropriate employee accountability policy to ensure that all personnel are held accountable for complying with cybersecurity policies and procedures.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Management should implement processes to ensure employees know and understand their 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 cybersecurity roles and responsibilities. For instance, employees may be required to review and signoff on 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 cybersecurity 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
- Cybersecurity training curriculum
- Cybersecurity training for developers
- 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.PL-2.1: The cybersecurity policy is supported by the organization's risk management program.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization should have a cybersecurity policy, standards, and procedures that align with the risk and complexity of the organization.

Describe how the organization establishes and implements its governance framework (e.g., via the enterprise risk management framework and the operational risk management framework). Include information on r risk and control taxonomy (or equivalent). Describe the organizational structure for the management and operation of cybersecurity enacted through policies and procedures as well as governance forums for the management of controls. Identify who owns/maintains cybersecurity policies and procedures and where they are located within the policy framework.

Examples of Effective Evidence

- Policy roadmap or process document, including document control to determine if/when policies are reviewed and updated
- Executive sign off for new and updated policies
- Communication plan for new and updated policies
- Copy of risk and control taxonomy to demonstrate alignment to policies
- Relevant Board or committee (e.g., Steering Committee, Governance Forum) meeting agendas and minutes (including attendees and roles)

GV.PL-2.2: Cybersecurity processes and procedures are established based on the cybersecurity policy.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Provide information on cybersecurity processes and procedures. Explain how the information and cybersecurity strategy integrates technology, policies, procedures, and training to mitigate risk. Describe how cybersecurity standards are defined, who reviews these standards, and what processes exist for updating standards. Show the taxonomy and relationship of policies, standards, and processes/procedures within the organization.

Examples of Effective Evidence

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

GV.PL-2.3: The cybersecurity policy is periodically reviewed and revised under the leadership of a designated Cybersecurity Officer (e.g., CISO) to address changes in the risk profile and risk appetite (e.g., new technologies, products, services, interdependencies, and the evolving threat environment).

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, ideally at least annually.

Describe responsibility, process, and frequency for reviewing/revising policies. As new or enhanced cybersecurity regulations are published (trigger event), or new cyber risks and threats are identified, show how policies are reviewed to ensure alignment or identify gaps (e.g., how trigger events 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

GV.PL-3.1: The cybersecurity policy, strategy and framework should take into account the organization's legal and regulatory obligations.

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.

Provide information on how new or enhanced cybersecurity regulations are published (trigger event), and how information security risk policies are reviewed to ensure regulatory alignment and identify gaps. Describe any existing efforts within the organization that may map regulatory requirements to existing policies, procedures, and controls. Provide information regarding any regulatory working groups that may oversee regulatory reviews/requests and exams with a cybersecurity scope.

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

GV.PL-3.2: The organization's cybersecurity policies are consistent with its privacy and civil liberty obligations.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

As referenced in GV.PL-3.1, the GLBA Interagency Guidelines Establishing Standards for Safeguarding Customer Information is the predominant legal expectation for financial institutions operating in the United States. Similar legislative and regulatory authorities include the General Data Protection Regulation (GDPR) in the EU, and the Monetary Authority of Singapore's "Technology Risk Management Guidelines." Additional regulatory guidance and/or legal requirements may apply based on products, services, legal structure, or geography, particularly as it relates to the intersection of personal information, privacy, data, and information security.

Provide information on how policies are designed in line with global standards, principles, and employee handbook and do not contradict local laws and regulations. Describe how policies are established (e.g., through a policy creation working group) and who signs off on policies (e.g., legal, HR). Describe how the information classification policy describes controls for the use and storage of information, as classified using an information classification schema, and are protected using access management and storage security controls.

Examples of Effective Evidence

- Applicable policies and standards (e.g., information classification, access controls, alignment with ethics and corporate compliance)
- Organization chart of privacy office
- Copy of the privacy notice sent to consumers and customers
- Tracking of acceptable use agreements signed by employees

GV.PL-3.3: The organization implements and maintains a documented policy or policies that address customer data privacy, and 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 documents.

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
- Matrix for data classification
- Organizational chart of privacy office, showing Chief Privacy Officer and reporting lines

Roles and Responsibilities (GV.RR)

GV.RR-1.1: The organization coordinates and aligns roles and responsibilities for personnel implementing, managing, and overseeing the effectiveness of the cybersecurity strategy and framework with internal and external partners.

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. If there are gaps, management should obtain the needed expertise by hiring, outsourcing, or improving cybersecurity training for current staff. Provide evidence of how the risk appetite is associated with cybersecurity and information security frameworks. Describe how cybersecurity risks are reported up to management, the Board, and/or risk or audit committees. Provide information on the formal governance structure in place to support the organization and change the programs as necessary. Include whether Steering Committees are in place for key projects. Describe how and where issues are escalated, documented, and tracked.

Provide information on the three lines of defense (or other model) and operational risk framework complimented with polices, standards, and guidance. Demonstrate how 2LoD provides advice, guidance, and challenge to cybersecurity programs in order to maintain controls towards the management of risks. Provide information on whether industry recognized standards are followed when measuring control effectiveness. Cite information from external third-party reviews, such as any maturity and cybersecurity control state assessments, to assess the maturity of the third party's cybersecurity capabilities. Provide detail on the Information security roles and responsibilities and job descriptions in place for cybersecurity (1LoD) and information security risk (2LoD).

Examples of Effective Evidence

- Organizational structure
- IT security responsibilities
- Cybersecurity job profiles
- Regional Risk Manager job profiles
- Cyber resilience capabilities 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

GV.RR-2.1: The organization has designated a 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.

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 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-2.2: 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 and authority. 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

GV.RR-2.3: 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 at least annually.

Describe how the CISO opines 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 key performance indicators (KPIs) and key risk indicators (KRIs)

GV.RR-2.4: The organization provides adequate resources to maintain and enhance the cybersecurity situational awareness of senior managers within the organization.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Situational awareness is considered foundational to effective cyber risk management. Describe how the organization provides adequate resources to maintain and enhance the cybersecurity situational awareness of senior managers throughout the entire organization. Cybersecurity situational awareness should be addressed from a program management perspective for all business functions within plans or policies. Resources to increase cybersecurity situational awareness may include briefings to business leadership (enterprise wide or by business line), table-top exercises, scenario testing, phishing exercises, workshops, or other centralized/decentralized training exercises.

Provide examples of such resources provided to senior management to maintain and enhance situational awareness for vulnerability management and incident response.

Refer to PR.AT-4.1 and PR.AT-4.2 for more information on situational cybersecurity awareness training for senior management.

Examples of Effective Evidence

- Senior management education for cybersecurity
- Examples of cybersecurity situational awareness training (e.g., briefing materials, table-top exercises, scenario testing, incident response training, workshops, phishing activities etc.)
- Results from cybersecurity situational awareness training (e.g., table-top meeting minutes)
- Completion tracking of cybersecurity awareness training for senior management
- Products, reports, notifications, or dashboards on cyber threat intelligence (e.g., threat intelligence dashboard)
- Meeting agendas and minutes, as applicable
- Comprehensive Capital Analysis and Review (CCAR) exercises

Security Program (GV.SP)

GV.SP-1.1: The organization has established, and maintains, a cybersecurity program designed to protect the confidentiality, integrity and availability of its information and operational systems, commensurate with the organization's risk appetite.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Describe how the cybersecurity program/Information Security Program is managed and governed. Provide examples on how the program assesses and manages 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 cybersecurity program's performance measures and risk indicators, and how the program addresses inherent risk to the organization. Describe how the program is reviewed and approved annually at the Board Risk Committee.

Describe how the organization strengthens the cybersecurity capability in line with organization's risk appetite and reduces the likelihood of a successful cyber-attack through any improvements. Provide examples of how programs of work align to industry recognized cyber frameworks and standards (e.g., the Profile, NIST, ISO, FFIEC CAT).

Examples of Effective Evidence

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

GV.SP-1.2: Based on a periodic risk assessment, the organization's cybersecurity program identifies and implements appropriate security controls to manage applicable cyber risks within the risk tolerance 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 conduct risk assessments to identify potential risks for all internet-based systems, internet facing systems, as well as those that process high-risk transactions.

Describe the cybersecurity program's process for identifying and tracking risks, and whether the current environment is operating within cyber risk tolerance levels (e.g., through risk assessments, key metrics, etc.). Provide information on the risk tolerance statements and governing authority that reviews and approves them.

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
- Key risk indicators (KRIs) and key performance indicators (KPIs) related to cyber risk tolerance levels

GV.SP-2.1: The organization implements a repeatable process to develop, collect, store, report, and refresh actionable cybersecurity key performance indicators and metrics.

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 failing to meet, meeting, or exceeding those established benchmarks.

Provide information on the effectiveness of cyber controls measured through a suite of cybersecurity key control indicators (KCI), key performance indicators (KPI), or key risk indicators (KRI) that were defined and mapped to controls. Additionally, describe KCI/KPI/KRI formal review process and roles of attendees in such review meetings. 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 the linkage to any improvement programs to uplift control 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

GV.SP-2.2: The organization develops, implements, and reports to management and the appropriate governing body (e.g., the Board or one of its committees) key cybersecurity performance indicators and metrics based on the cyber risk strategy and framework to measure, monitor, and report actionable indicators to help guide the security program.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

The organization should use cybersecurity metrics to determine where weaknesses or gaps exist within the cybersecurity program. The metrics can then be used to identify trends, make strategic decisions to address those trends, and allocate funding appropriately. 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 key risk indicators (KRIs) and key control indicators (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 cyber 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)
- Monthly cyber dashboards
- Maturity model or methodology used to align KPIs and metrics

GV.SP-2.3: 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 cybersecurity strategy and how it was developed, including the objectives and assessments to identify benchmarks and associated maturity levels. Describe how the organization identifies areas for improvement and measures the cybersecurity program 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 key risk indicators (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

Independent Risk Management Function (GV.IR)

GV.IR-1.1: The organization's enterprise-wide cyber risk management framework includes an independent risk management function that provides assurance that the cyber risk management framework is implemented as intended.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Enterprise risk management objectives and actions encompass 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 operational risk management framework and the three lines of defense pertain to an independent risk management function that provides assurance that the cyber 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 cyber 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-1.2: An independent risk management function 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 cyber risk management framework.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Describe the operational risk management framework and how the three lines of defense create 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 cyber risk management framework. Provide examples of independence.

Examples of Effective Evidence

- Cyber dashboards
- 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-1.3: The independent risk management function has appropriate understanding of the organization's structure, cybersecurity program, 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 appropriate understanding of the organization's structure, 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-1.4: Individuals responsible for independent risk management and oversight are independent of business line management, including senior leadership.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Describe how the operational risk management framework and the three lines of defense allow for an independent risk management function that is independent of business line management, including senior leadership. 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

- Risk control assessment information and cyber risk events reporting
- Service catalog
- Organizational chart

GV.IR-2.1: An independent risk management function assesses the appropriateness of the cyber risk management program according to the organization's risk appetite.

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 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 cyber 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-2.2: An independent risk management function frequently and recurrently assesses the organization's controls and cyber risk exposure, identifies opportunities for improvement based on assessment results, and proposes risk mitigation strategies and improvement actions when needed.

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 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-3.1: An independent risk management function reports to the appropriate governing authority (e.g., the Board or one of its committees) and to the appropriate risk management officer within the organization on the implementation of the cyber risk management framework throughout the organization.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

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.

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. Describe how 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-1.1: The organization has an independent audit function.

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.

Examples of Effective Evidence

- Internal audit charter(s)
- Audit instruction manual

GV.AU-1.2: The organization has an independent audit plan that provides for an evaluation of the organization's compliance with the appropriately approved cyber risk management framework and its cybersecurity policies and processes including how well the organization adapts to the evolving cyber 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 cyber risk and cybersecurity is covered by internal audit teams through various audits. Audits should address the effectiveness of the 1LoD and 2LoD activities for managing and controlling cyber 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 cybersecurity as a 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

GV.AU-1.3: An independent audit function tests security controls and information security policies.

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. Cybersecurity 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-1.4: 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 as per internal audit's audit methodology.

Examples of Effective Evidence

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

GV.AU-2.1: A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across the sector.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

Provide information on how internal audit updates its assessment of cyber risks based on its continuous monitoring process and audit universe coverage. Describe how the audit plan is 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

GV.AU-2.2: A formal process is in place for the independent audit function to update its procedures based on changes to the organization's risk appetite and risk tolerance.

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. The cyber 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 cyber risks based on its continuous monitoring process. When necessary, describe how the independent audit function adjusts the audit plan to ensure sufficient audit coverage.

Examples of Effective Evidence

- Audit instruction manual
- Supporting internal audit plans and reports

GV.AU-3.1: An independent audit function reviews 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 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-3.2: An 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-3.3: An independent audit function reports to the appropriate 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 cyber 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 appropriate 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. While important to note when the cyber risk tolerance has been exceeded it should be addressed by the independent risk management function rather than the independent audit function. Regardless, when the risk tolerance is exceeded, the appropriate governing authority should be notified.

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

Technology (GV.TE)

GV.TE-1.1: The organization identifies how cybersecurity will support emerging technologies that support business needs (e.g., cloud, mobile, IoT, IIoT, etc.) by integrating cybersecurity considerations into the lifecycle of new technologies from their inception.

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 controls to defend against these threats. Describe how analysis in conjunction with risk quantification determines the most effective controls in order to mitigate these threats. Describe how cybersecurity activities, such as appropriate risk assessment and cybersecurity 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 cyber risk programs, updating of policies, and standards.

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.TE-1.2: The organization applies its cyber risk management framework to all technology projects.

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 independent risk function (e.g., 2LoD) provides oversight and challenge on high risk and strategic change initiatives. Describe how all projects follow a documented framework and how the framework assists project managers and project 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)

GV.TE-2.1: 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 system development lifecycle (e.g., SABSA, NIST 800-53, ISO 27001, etc.) Describe how these are defined and maintained. Provide examples.

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.)

IDENTIFY

Asset Management (ID.AM)

ID.AM-1.1: 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 key risk indicators (KRIs) / key performance indicators (KPIs), on the efficiency and effectiveness of the asset management program
- Related process flows

ID.AM-2.1: The organization maintains a current and complete inventory of software platforms and business applications.

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-1.1 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 and patches. 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 key risk indicators (KRIs) / key performance indicators (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-3.1: The organization maintains an inventory of internal assets and business functions, that includes mapping 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 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
- Related dashboards, inclusive of key risk indicators (KRIs) / key performance indicators (KPIs), and compliance documentation

ID.AM-3.2: The organization maintains a current and complete inventory of types of data being created, stored, or processed by its information assets.

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). 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 and tools 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

CYBER RISK INSTITUTE

ID.AM-3.3: The organization's asset inventory includes maps of network resources, as well as connections with external and mobile resources.

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, 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-4.1: The organization maintains an inventory of external information systems.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization (e.g., remote access from personally owned devices, privately owned computing and communications devices, cloud services, etc.). 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 information systems
- Diagrams or connectivity flow documentation
- External systems point of contact information

ID.AM-5.1: The organization implements and maintains a written risk-based policy or policies on data governance and classification, approved by a Senior Officer or the organization's governing body (e.g., the Board or one of its committees).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

The organization should have policies to govern the inventory and classification of data resources.

Describe the approved policies 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, including review and approval by the appropriate Senior Officer or governing body.

Examples of Effective Evidence

- Data policy inventory
- Data policy governance and oversight meeting agendas and minutes
- Data governance roles and responsibilities (e.g., Privacy Officer, Compliance Officer, etc.)
- Documentation of data policy review/evaluation and approval (e.g., quarterly or annually)
- Information classification matrix/guidance for classifying data

ID.AM-5.2: The organization's resources (e.g., hardware, devices, data, and software) are prioritized for protection based on their sensitivity/classification, criticality, vulnerability, business value, and importance to the organization.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

As referenced in ID.AM-5.1, the organization implements and maintains a policy on data governance and classification. Classification enables the organization to determine the sensitivity and criticality of resources and prioritize assets according 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-6.1: Roles and responsibilities for the entire cybersecurity workforce and directly managed third-party personnel are established, well-defined and aligned with internal roles and responsibilities.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Organizational structure, roles, responsibilities, and levels of authority of the cybersecurity workforce should be clearly established and well-defined especially regarding roles required to handle sensitive data. The organization's management may rely on third parties to provide critical services. In these instances, the roles of directly managed third-party personnel should also be established and well-defined.

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 directly-managed third-party personnel. 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
- 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)

Risk Assessment (ID.RA)

ID.RA-1.1: The organization's business units identify, assess and document applicable cyber risks and potential vulnerabilities associated with business assets to include workforce, data, technology, facilities, service, and IT connection points for the respective unit.

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 applicable cyber risks and potential vulnerabilities. Describe how the business units' (lines of business) assessments of cyber risks and vulnerabilities link to, or are associated with, business assets, workforce, data, technology, facilities, service, and IT connection points. Describe how the business unit assessments of cyber risks and vulnerabilities link to the enterprise assessment of cyber risks and vulnerabilities. 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-2.1: The organization participates actively (in geopolitical alignment with its business operations) in applicable 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-3.1: The organization identifies, documents, and analyzes 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 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 a process to gather and analyze relevant cyber threat information.

Describe the framework and processes used within the organization to identify, document, and analyze internal and external threats to the organization.

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

ID.RA-3.2: The organization includes in its threat analysis those cyber threats which could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred in the past.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

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. Threat information is correlated to an organization's vulnerabilities and other factors to provide the organization with a risk calculation. Threat information is integrated with intrusion prevention, intrusion detection, and data loss prevention technologies to provide alerts and real-time remediation of threat activity.

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

ID.RA-3.3: The organization regularly reviews and updates results of its cyber threat analysis.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

As referenced in ID.RA-3.1, 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 this analysis.

Provide information on how the organization regularly reviews and updates the results of its cyber threat analysis.

Examples of Effective Evidence

- Cyber threat 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
- Red team/purple team testing documentation, including plans, and resulting reports
- Threat catalogs

ID.RA-4.1: The organization's risk assessment approach includes identification of likelihood and potential business impact of applicable cyber risks being exploited.

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 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
- 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-5.1: Cyber threats, vulnerabilities, likelihoods, and impacts are used to determine overall cyber risk to the organization.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

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 cyber risk to the organization. Integration and analysis of threat intelligence should inform the organization's decision-making regarding cyber risk reduction activities.

Provide information showing cyber threat, vulnerability, likelihood, and impact assessments are linked to the overall evaluation of cyber risk to the organization.

Examples of Effective Evidence

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

ID.RA-5.2: The organization considers threat intelligence received from the organization's participants, service and utility providers and other industry 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 partners, service and utility providers, and other industry organizations are reviewed, analyzed, aggregated, and considered as part of threat intelligence.

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

ID.RA-5.3: 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-5.4: The organization's business units assess, on an ongoing basis, the cyber risks associated with the activities of the business unit.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Cyber 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 cyber risk (i.e., risk governance framework, control assessments, etc.) and any models or frameworks used for the assessment.

Examples of Effective Evidence

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

ID.RA-5.5: The organization tracks connections among assets and cyber risk levels throughout the life cycles of the assets.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Response Guidance

Provide information as to how the organization tracks connections (e.g., at the electronic transmission, data, function, and service levels) among assets and cyber risk levels throughout the life cycle of the assets. Describe how application instance to application instance interfaces are tracked in inventory including information on the transfer of data. Describe how and where IT service-to-service dependency relationships are managed. Provide information on software and hardware version lifecycles and how those are maintained in inventory.

Critical services are defined and any associated external connectivity is reflected in a network diagram or topology. Management should prepare a listing of all critical services (and the respective third-party vendor) where an external connection is necessary for the service to be provided (e.g., core system, mortgage processing, Bank Secrecy Act monitoring).

Examples of Effective Evidence

- Vulnerability management framework and reporting
- Asset evergreening standard
- Evergreening reports (hardware and software)
- Security risk assessments
- Critical services guide
- Data flow diagrams

ID.RA-5.6: The organization determines ways to aggregate cyber risk to assess the organization's residual cyber risk.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Describe how cyber risks are aggregated, mitigated, transferred or accepted to assess the organization's residual cyber risk. Provide information on metrics and dashboards prepared for different audiences (e.g., higher level for board and senior management, more detailed for working groups, etc.), including assessment results, risk treatments, risk behaviors and infrastructure security. Provide information on cyber risk management/measurement framework.

Examples of Effective Evidence

- Cyber risk metrics and dashboards prepared for different audiences
- Related committee meeting agendas and minutes
- Risk program supporting documentation
- Related policies and standards
- Related framework or program information
- Risk impact reports
- Enterprise risk strategy including risk mitigation, risk transfer and acceptance processes
- Risk Register
- Processes and procedures used for aggregating and assessing cyber risk

ID.RA-6.1: 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

- Key risk indicators (KRIs) and key performance indicators (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-6.2: Independent risk management is required to analyze cyber risk at the enterprise level to identify and ensure effective response to events with the potential to impact one or multiple operating units.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Describe the independent risk management framework and related functions utilized to analyze cyber risk at the enterprise level (i.e., 2LoD activities, examined by 3LoD, to ensure that risk management activities are working effectively).

Examples of Effective Evidence

- Operational risk and control framework
- Committee meeting agendas and minutes
- Risk and control assessments, their frequency and coverage, and related organization charts and reporting
- Threat management framework
- Board reports
- Audit plan and audit reports
- Consultants' reports
- Vulnerability and penetration tests

CYBER RISK INSTITUTE

PROTECT

Identity Management and Access Control (PR.AC)

PR.AC-1.1: Physical and logical access to systems is permitted only for individuals who have a legitimate business requirement and have been authorized.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Least privilege refers to the security objective of granting users only the level of access they need to perform their official duties. For example, data entry clerks may not have any need to run analysis reports of their database, nor would they have need to go into a data center to physically administer infrastructure servers. For a core processing system, roles and privileges are typically defined based on templates and common job descriptions such as teller, loan officer, collection manager, etc. Where feasible, staff that performs accounting functions and makes general ledger entries should not be able to perform transactions on customer accounts. The organization's management should ensure all users are identified and authenticated when accessing systems, applications, and hardware.

Provide information regarding the physical and logical access controls that demonstrate that access is only permitted to individuals who have a legitimate business requirement and have been authorized.

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

PR.AC-1.2: User access authorization is limited to individuals who are appropriately trained and monitored.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

User access authorization is the process for ensuring that every user that accesses an information system for processing, storing, or transmitting information is cleared and authorized to view that data. Training and monitoring should be commensurate with the sensitivity and criticality of the information accessible by the user.

Provide information on how user access authorization, for physical and logical access, is limited to individuals who are appropriately 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

- Computer system access control policy and procedure
- Access request and review standard
- Authentication security standard
- Access recertification/revocation guidelines
- Additional training for business and privileged access risks commensurate with the level of responsibility
- Training requirements and history of training completion (i.e., course records)
- Job aids/trainings for individuals assigned to perform access authorization

PR.AC-1.3: Identities and credentials are actively managed or automated for authorized devices and users (e.g., removal of default and factory passwords, revocation of credentials for users who change roles or leave the organization, 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. 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. 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. 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
- 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.AC-2.1: The organization manages and protects physical access to information assets (e.g., session lockout, physical control of server rooms).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization should 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 and protects physical access to information assets.

Examples of Effective Evidence

- Physical access controls policy
- 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 thumbdrives)

PR.AC-3.1: Remote access is actively managed and restricted to necessary systems.

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.

Describe how remote access is actively managed and restricted to necessary systems. Necessary systems may include components, applications and/or devices.

Examples of Effective Evidence

- Computer system access control policy
- Network security standard
- Various system security documentation
- User access review (VPN, PIN logon, etc.)
- Remote access and/or telecommuting security policy and procedures

PR.AC-3.2: The organization implements multi-factor authentication, or at least equally secure access controls for remote access, if it is warranted by applicable risk considerations.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization should secure remote access to and from their critical systems. Multi-factor authentication (MFA) is a security control that requires more than one authenticating element to verify the user's identity (e.g., something known, something the user has, or something they are). MFA could be in the form of software tokens, organization issued certificates, hardware tokens, biometrics, or various other forms.

Describe how the organization implements multi-factor authentication or equally secure access controls for remote access. Provide rationales and documentation for the risk-based decisions regarding the use or non-use of MFA.[13]

Examples of Effective Evidence

- Computer system access control policy, standard, and procedures
- 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.

[13] See NIST Special Publication 800-63 Rev. 3 or ISO 27001 Annex A.9 for risk-based usage of authentication tools.

PR.AC-4.1: The organization limits access privileges to the minimum necessary.

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.

Provide information regarding how the organization limits access privileges to the minimum necessary.

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

PR.AC-4.2: The organization institutes strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization should provide the necessary reviews and authorization (approval) for privileged access when requested. 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.

Provide information on how the organization institutes controls over privileged system access by strictly limiting and closely supervising staff 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.AC-4.3: The organization institutes control 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. 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

PR.AC-5.1: Networks and systems are segmented to maintain appropriate security.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization should ensure networks and systems 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 and systems are segmented to maintain appropriate security.

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.AC-5.2: The organization controls access to its wireless networks and the information that these networks process by implementing appropriate mechanisms (e.g., strong authentication and transmission controls, 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.

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

PR.AC-6.1: The organization authenticates identity and validates the authorization level of a user before granting access to its systems.

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 and validates the authorization level of a user before granting access to its systems.

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.AC-7.1: The organization performs a risk assessment for prospective users, devices and other assets which authenticate into its ecosystem with a specific focus on:

TIER 1	TIER 2	TIER 3	TIER 4
✓			

(1) The type of data being accessed (e.g., customer PII, public data);

(2) The risk of the transaction (e.g., internal-to-internal, external-to-internal);

(3) The organization's level of trust for the accessing agent (e.g., external application, internal user); and

(4) The potential for harm.

Response Guidance

Risk assessments help organizations identify high-risk devices or assets.

Provide information on how the organization performs risk assessments on prospective users, devices, and other assets which authenticate into its ecosystem. 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 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.

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.AC-7.2: Based on the risk level of a given transaction, the organization has defined and implemented authentication requirements, such as including implementing multi-factor, out-of-band authentication for high risk transactions.

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 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 or connection, the organization has defined and implemented appropriate authentication requirements, such as implementing multi-factor authentication for high risk transactions.

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

Awareness and Training (PR.AT)

PR.AT-1.1: All personnel (full-time or part-time; permanent, temporary or contract) receive periodic cybersecurity awareness training, as permitted by law.

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.

Provide situational awareness training that is relevant to all personnel (full-time or part-time; permanent, temporary or contract) on an annual or more frequent schedule. Prescribed training should be scoped and defined for areas where additional job-relevant requirements warrant additional validation. Provide information on any exceptions.

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

PR.AT-1.2: Cybersecurity awareness training includes at a minimum appropriate awareness of and competencies for data protection, detecting and addressing 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, detecting and addressing 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
- Examples of training

PR.AT-1.3: Cybersecurity awareness training is updated on a regular basis to reflect risks identified by the organization in its risk assessment.

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 identified by the organization in its risk assessment. 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
- 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-2.1: High-risk groups, such as those with privileged system access 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, database administrators, or business unit personnel, 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., Business Email Compromise, insider threats, etc.).

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-2.2: Cybersecurity personnel receive training appropriate for their roles and responsibilities in cybersecurity, including situational awareness training sufficient to maintain current knowledge of cyber threats and countermeasures.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization's management should establish minimum standards and certifications for cybersecurity personnel and require continuing specialized education to ensure expertise is maintained. Cybersecurity training should be current and relevant. As cybersecurity threats change, training should be adopted to address the changing threat landscape.

Describe how cybersecurity personnel receive cybersecurity training that is appropriate for their roles and responsibilities and addresses cybersecurity risks and changing cybersecurity threats and countermeasures. Provide information on the content of situational awareness materials and how 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

- Certification requirements for cybersecurity personnel
- 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-2.3: A mechanism is in place to verify that key cybersecurity personnel maintain current knowledge of changing cyber threats and countermeasures.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Key cybersecurity personnel depend on the specific organization, but may include workforce involved in information security functions such as operations, enterprise architecture, application development, etc. Cybersecurity 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, processes, or threats. Describe which metrics and reporting mechanisms are in place to verify that key cybersecurity personnel maintain current knowledge of changing cyber threats and countermeasures.

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-3.1: The organization has established and maintains a cybersecurity awareness program through which the organization's customers are kept aware of 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. One method for informing customers and stakeholders of cybersecurity risks is to provide information on the organization's website (e.g., security requirements that customers should follow).

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 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 social media programs / documentation
- Annual review of customer awareness training

PR.AT-3.2: Cybersecurity training provided through a third-party service provider or affiliate should be consistent with the organization's cybersecurity policy and program.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Provide information on how the organization assesses courses and training offerings provided by third-party suppliers. Describe how the organization implements agreements with third-party training providers for selected courses and materials. Provide detail on how all cybersecurity training offerings are designed and managed as part of the cybersecurity training and situational awareness program.

Examples of Effective Evidence

- Organizational cybersecurity training objectives, policies, and program
- Cybersecurity training schedule and materials
- Training-related description of services provided by training team
- Examples of training
- Third-party contracts detailing responsibilities and service level agreements
- Third-party vendor policy and/or procedure document

PR.AT-3.3: Cybersecurity training covers topics designed to minimize risks to or from interconnected parties.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Provide information as to how cybersecurity training covers topics designed to minimize risks to or from interconnected parties. For example, training on the effective use of multifactor authentication, limited access based upon role, classification of data, etc.

Examples of Effective Evidence

- Cybersecurity training documents
- Cybersecurity situational awareness materials
- Training and situational awareness delivery schedule
- Related training samples
- Third-party cybersecurity training policy, standards, and procedures

PR.AT-4.1: 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-4.2: 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 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) 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

PR.AT-5.1: The individuals who fulfill the organization's physical and cybersecurity objectives (employees or outsourced) have been informed of 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 cybersecurity operations and 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 physical and cybersecurity employees 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

Data Security (PR.DS)

PR.DS-1.1: Data-at-rest is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy.

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 is necessary to protect data from unauthorized access or theft.

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. 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 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

PR.DS-1.2: Controls for data-at-rest include, but are not restricted to, appropriate encryption, authentication and access control.

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 is necessary to protect data from unauthorized access or theft. Securing user information begins with a proper understanding of security controls and the protection of user passwords or authentication mechanisms. 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 communications containing passwords or transmitting cryptographic password hashes instead of plaintext passwords help protect against threats to capture passwords.

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

- Cryptography and key management standard
- Cryptographic algorithms standard
- Managing electronic Information security standard
- Encryption systems and key management documentation
- Authentication security standard
- Access request and review security standard
- Mobile device standards (laptop, removable media)

PR.DS-2.1: Data-in-transit is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy.

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.

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

PR.DS-2.2: Controls for data-in-transit include, but are not restricted to, appropriate encryption, authentication and access control.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization should identify and classify confidential data held internally and residing at third parties as a standard part of data management practices. Management should understand how that data is used, exchanged, and transmitted, and encrypt all confidential data-in-transit on public or untrusted networks.

Provide information in support of controls for data-in-transit including, but not restricted to, appropriate encryption, authentication, and access control. 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
- Cryptography and key management standard
- Cryptographic algorithms standard
- Managing electronic Information security standard
- Secure use of removable storage devices
- Network security standard
- Windows client endpoints security standard
- Site-to-site VPN configuration standards
- TLS and SecureMail Description

PR.DS-3.1: The organization has an asset management process in place and assets are formally managed (e.g., in a configuration management database) throughout removal, transfers, end-of-life, and secure disposal or re-use of equipment processes.

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.

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.

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

PR.DS-4.1: The organization maintains appropriate system and network availability, consistent with business requirements and risk assessment.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Provide information on how the organization maintains appropriate system and network availability. 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

PR.DS-5.1: 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-6.1: The organization uses integrity checking mechanisms to verify software, firmware and information integrity, as practicable.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Describe how the organization uses information security integrity checking mechanisms to verify the integrity of software, firmware, and other information. Provide information on the various mechanisms in place and how they are used for software, firmware, and information integrity. 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

PR.DS-7.1: The organization's development, testing and acceptance environment(s) are separate from the production environment, and test data is protected and not used in the production environment.

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 development, testing and acceptance environment(s) are separate from the production environment (logically/physically). Provide information on the network segmentation. Describe how data (both test and production) is protected, managed, and not used in inappropriate environments.

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

PR.DS-8.1: The organization uses integrity checking mechanisms to verify hardware integrity, as practicable.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Response Guidance

Describe how the organization uses integrity checking mechanisms to verify hardware integrity, as practicable. 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, and information integrity.

Examples of Effective Evidence

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

Information Protection Processes and Procedures (PR.IP)

PR.IP-1.1: The organization establishes and maintains baseline system security configuration standards to facilitate consistent application of security settings to designated information assets.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

The organization should develop baseline security configuration standards for production systems and others 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 and industry standards. Describe how the baseline security configuration standards facilitate consistent application of security settings to designated information assets.

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.IP-1.2: The organization establishes policies, procedures and tools, such as policy enforcement, device fingerprinting, patch status, operating system version, level of security controls, etc., to manage personnel's mobile devices before allowing access to the organization's network and resources.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

The organization should establish a mobile device management system to monitor and manage all mobile devices that connect to the internet. Defending mobile and remote machines against the latest known threats involves solutions that verify that the necessary fixes or patches are in place and that the machines comply with corporate policies. For example, organizations may require that machines have up-to-date antivirus software. Mobile device encryption, using either hardware or software-based solutions, is a way to secure data on smartphones, tablets, and mobile devices against the loss of information due to a loss or theft of the device. Organizations should ensure any mobile device storing or accessing confidential information has implemented an effective encryption solution.

Describe how the organization establishes policies, procedures, and tools to manage personnel's mobile devices before allowing access to the organization's network and resources. Provide information related to policy enforcement, device fingerprinting, patch status, operating system version, level of security controls, and other methods where applicable.

Examples of Effective Evidence

- Mobile device security policy and standard
- Device protection documentation including encryption or sandbox requirements
- Mobile device management procedures, including patch management, integrity scanning (e.g., jailbreak detection) and remote wipe capabilities
- Control procedures to prevent unauthorized or rogue devices from connecting to internal networks
- Mobile dashboard reporting
- Related reporting (e.g., inventory, permission reports, and exception reporting)
- Use of equipment security policy and standard

PR.IP-1.3: The organization performs regular enforcement checks to ensure that non-compliance with baseline system security standards is promptly rectified.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Response Guidance

Describe how the organization performs regular enforcement checks to ensure that non-compliance with baseline system security standards is promptly rectified, in accordance with their risk. Provide information on the 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.IP-2.1: The organization implements a process for Secure System Development Lifecycle for in-house software design and development.

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.

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 and development.

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

PR.IP-2.2: The organization implements a process for evaluating (e.g., assessing or testing) externally developed applications.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

The organization's management should establish a formal process and/or procedure for evaluating externally developed applications.

Provide information on the process used within the organization to evaluate (e.g., assessing or testing) externally developed applications.

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

PR.IP-2.3: The organization assesses the cyber risks of software prior to deployment.

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 (e.g., penetration testing).

Describe how the organization assesses the cyber risks of software prior to deployment. Provide information on the assessment process and any tools used.

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

PR.IP-3.1: The organization's change management process explicitly considers cyber risks, in terms of residual cyber risks identified both prior to and during a change, and of any new cyber risk created post-change.

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. To ensure cybersecurity risks and vulnerabilities are not introduced with changes, the change management process needs to include a security impact or similar analysis.

Describe how the organization's change management process explicitly considers cyber risks, in terms of residual cyber risks identified both prior to and during a change, and of any new cyber risk created post-change. Provide information related to the change management process and cyber risks.

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
- Related documentation (e.g., possibly change tickets)

PR.IP-4.1: The organization designs and tests its systems and processes to enable recovery of accurate data (e.g., material financial transactions) sufficient to support normal operations and obligations following a cybersecurity incident.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Describe how the organization designs and tests its systems and processes to enable recovery of data (e.g., material financial transactions) sufficient to support normal operations and obligations following a cybersecurity incident. 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.

PR.IP-4.2: The organization conducts and maintains backups of information and periodically conduct tests of backups to business assets (including full system recovery) to achieve cyber resilience.

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'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 conducts and maintains backups of information. Describe how the organization periodically conducts tests of backups to business assets (including full system recovery) to support cyber resilience. 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

PR.IP-4.3: 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

PR.IP-4.4: Recovery point objectives to support data integrity efforts are consistent with the organization's resumption time objective for critical operations.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Describe how the organization's recovery point objectives to 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 recovery time objectives (RTO) and recovery point objectives (RPO)
- Business and system impact assessments identifying critical-operations service level agreements and RTO/RPO objectives
- Service continuity planning standards, processes, and plans
- Related testing documentation
- Business continuity/resiliency plans

PR.IP-5.1: 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

PR.IP-6.1: Data is maintained, stored, retained and destroyed according to the organization's data retention policy.

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

PR.IP-7.1: A formal process is in place to improve protection processes by integrating lessons learned and responding to changes in the organization's environment.

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 processes by integrating lessons learned and responding to changes in the organization's environment. 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

PR.IP-8.1: The organization shares appropriate types of information about the effectiveness of its protective measures with appropriate parties.

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. Proactively sharing threat intelligence helps organizations achieve broader cybersecurity situational awareness among external stakeholders.

Describe how the organization shares appropriate types of information about the effectiveness of its protective measures 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 for sharing information.

Examples of Effective Evidence

- Organizational information
- Cyber threat and intelligence report samples
- Incident management policies, procedures, and communication templates
- Key law enforcement and regulatory contacts identified and maintained
- Cyber threat and intelligence analysis samples
- Evidence of membership in industry associations and/ or information sharing organizations
- Contracts with trusted parties, if applicable
- Information sharing examples
- Organizational charts for teams, roles, and responsibilities
- Maturity documentation for protective measures

PR.IP-9.1: The organization's business continuity, disaster recovery, crisis management and response plans are in place and managed.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization should have Board-approved business continuity, disaster recovery, crisis management, and data backup/response plans in place to recover operations following an incident. A business continuity plan should address: business impact analysis and risk assessment, alternate processing for critical business functions while systems/applications and facilities are unavailable, recovery strategies and procedures for critical systems, roles and responsibilities, and business continuity and disaster recovery testing.

Describe how the organization's business continuity (business process), disaster recovery (data center process), crisis management (business process), and incident response plans (cybersecurity process) are in place, coordinated and managed.

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

PR.IP-9.2: The organization defines objectives for resumption of critical operations.

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). 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 plans, policies, and procedures
- Recovery time objectives
- Recovery point objectives
- Critical operations inventory
- Roles and responsibilities for staff involved in resumption of critical operations
- Recent business impact analysis

PR.IP-10.1: 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 clients.

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. 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 clients.

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

PR.IP-10.2: The organization's testing program validates the effectiveness of its cyber resilience framework on a regular basis.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

As referenced in PR.IP-10.1, the organization establishes testing programs that include a range of scenarios.

Describe how the organization's testing program validates the effectiveness of its cyber resilience framework on an annual or more frequent basis and according to the risk profile of the organization. Provide information on the organization's testing framework and strategy. Describe the types of testing performed.

Examples of Effective Evidence

- Business continuity/resiliency plans, policies and procedures
- Network penetration testing strategy
- Application security testing strategy
- Targeted test results and reports
- Security assessments

PR.IP-10.3: The organization's governing body (e.g., the Board or one of its committees) is involved in testing as part of a crisis management team and is informed of test results.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Response Guidance

Describe how the organization's governing body is 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 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

PR.IP-10.4: The organization promotes, designs, organizes and manages testing exercises designed to test its response, resumption and recovery plans and processes.

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 response, resumption, recovery plans, and processes. Include information on how the organization shares results of testing exercises to staff and management, such as through metrics or board reporting.

Examples of Effective Evidence

- Business continuity/resiliency plans, policies, and procedures
- Roles and responsibilities of staff involved in testing exercises
- Evidence of all tests conducted in the past 12 months for business continuity / disaster recovery
- Results of testing exercises, including metrics or board reporting
- Incident or crisis management plans, policies, and procedures
- 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

PR.IP-11.1: The organization conducts background/screening checks on all new employees, as permitted by law.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization should conduct background verifications for prospective employees with access to confidential or sensitive data, systems, or facilities.

Describe how the organization conducts background/screening checks on all new 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

PR.IP-11.2: The organization conducts background/screening checks on all staff at regular intervals throughout their employment, commensurate with staff's access to critical systems or a change in role, as permitted by law.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

Describe how the organization conducts background/screening checks on all staff at regular intervals throughout their employment, commensurate with staff's access to critical systems or a change in role, as permitted by law. 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 vetting standards utilized including the program's purpose, scope, responsibilities, etc. Provide information on how the program meets applicable regulatory requirements. Provide information on additional background checks performed for uses in specific roles that go beyond the standard background/screening validation.

Examples of Effective Evidence

- 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

PR.IP-11.3: The organization establishes processes and controls to mitigate cyber risks related to employment termination, as permitted by law.

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. 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.

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

PR.IP-12.1: The organization establishes and maintains capabilities for ongoing vulnerability management, including systematic scans or reviews reasonably designed to identify publicly known cyber vulnerabilities in the organization based on the risk assessment.

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 or reviews reasonably designed to identify publicly known cyber vulnerabilities in the organization based on a risk assessment. Describe how the organization determines eligibility 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.

Examples of Effective Evidence

- Vulnerability management security standards and procedures, including eligibility
- Risk assessment criteria
- Related reporting (dashboards)
- Organizational structure, including roles and responsibilities for vulnerability management
- 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

PR.IP-12.2: The organization establishes a process to prioritize and remedy issues identified through vulnerability scanning.

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 is normally conducted on a routine basis.

Describe what processes the organization has established to prioritize and remedy issues identified through vulnerability scanning. Describe the prioritization methodology, such as potential impact, time to remedy, etc., and the process for vulnerability scanning.

Examples of Effective Evidence

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

PR.IP-12.3: The organization has a formal exception management process for vulnerabilities that cannot be mitigated due to business-related exceptions.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Provide information on the organization's formal 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

PR.IP-12.4: The organization ensures that a process exists and is implemented to identify patches to technology assets, evaluate patch criticality and risk, and test and apply the patch within an appropriate time frame.

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 them in a segregated environment, and to install them when appropriate.

Describe the implemented process used to identify patches to technology assets, evaluate patch criticality, and risk, and test and apply the patch within an appropriate time frame. 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.)

Maintenance (PR.MA)

PR.MA-1.1: Policies, standards and procedures for the maintenance of assets include, but are not limited to, physical entry controls, equipment maintenance and removal of assets.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

Describe the policies, standards, and procedures in place for the maintenance of 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, equipment maintenance, removal of assets, and related controls are in place.

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

PR.MA-2.1: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

Describe how the remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access. Describe the supporting processes and tools that are in place along with roles and responsibilities.

Examples of Effective Evidence

- 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
- Inventory of assets
- Asset maintenance logs or other metrics

Protective Technology (PR.PT)

PR.PT-1.1: The organization's audit trails are designed to detect cybersecurity events that may materially harm normal operations of the organization.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

An audit trail is a record showing who has accessed an information system and what operations the user has performed during a given period.

Describe how audit trails have been designed to detect cybersecurity events that may materially harm normal operations of the organization. Provide information regarding the structure of audit trails. Describe how audit trails (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.PT-1.2: The organization's activity logs and other security event logs are reviewed and are retained in a secure manner for an appropriate amount of time.

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 reviewed and retained in a secure manner for an appropriate amount of time. Provide information on the review process. Provide information on the storage and length of time event logs are stored.

Examples of Effective Evidence

- Security event logging and monitoring policy, standard, and procedure
- 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

PR.PT-2.1: The organization's removable media and mobile devices are protected and use is restricted according to policy.

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's removable media and mobile devices are protected. Describe how removable media and mobile device use is restricted according to the organizations policies or procedures 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)

PR.PT-3.1: 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.[14] The organization should securely configure network components 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

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

PR.PT-4.1: The organization's communications and control networks are protected through applying defense-in-depth principles (e.g., network segmentation, firewalls, physical access controls to network equipment, etc.).

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.

Describe how the organization's communications and control networks are protected through application of defense-in-depth principles. Provide information regarding network segmentation (strategy and method), firewalls, physical access controls to network equipment, and other related controls, as applicable.

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

PR.PT-5.1: The organization implements mechanisms (e.g., failsafe, load balancing, hot swap) 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) to achieve resilience requirements in normal and adverse situations. 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

DETECT

Anomalies and Events (DE.AE)

DE.AE-1.1: The organization identifies, establishes, documents and manages a baseline mapping of network resources, expected connections and data flows.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Organizations should maintain network and data flow diagrams that 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 mapping of network resources, expected connections and data flows.

Provide information supporting mapping of resources, connections, and data flows.

Examples of Effective Evidence

- Inventory of network resources and network connections
- 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

DE.AE-2.1: The organization performs timely collection of relevant data, as well as advanced and automated analysis (including use of security tools such as antivirus, IDS/IPS) on the detected events to:

(1) Assess and understand the nature, scope and method of the attack;

(2) Predict and block a similar future attack; and

(3) Report timely risk metrics.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

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 relevant 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-3.1: The organization has a capability to collect, analyze, and correlate events data across the organization in order to predict, analyze, and respond to changes in the operating environment.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

The organization should have capabilities in place to collect, analyze, and correlate events data. 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 how the organization collects, analyzes, and correlates events data across the organization in order to predict, analyze, and respond to changes in the operating environment. Provide information regarding the threat intelligence structure and process.

Examples of Effective Evidence

- Event logging and monitoring policy, standard, and procedure
- Security incident response standard
- Documents on mechanisms or tools in place (e.g., log repository and correlation, event management, incident response management, etc.)
- Documents showing that incidents are classified, logged, and tracked
- Event detection and correlation metrics (monthly, quarterly, or annually) are analyzed to understand attack targets and methods
- Incident response metrics and examples
- Related reporting

DE.AE-3.2: The organization deploys tools, as appropriate, to perform real-time central 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.

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 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-4.1: The organization has a documented process in place to analyze the impact of a material cybersecurity incident (including the financial impact) on the organization as well as across the financial sector, as appropriate, per organization's size, scope, and complexity and its role in the financial sector.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

The organization should have processes in place for analyzing the material impact associated with cybersecurity incidents. The materiality 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.[15]

Describe the documented process in place to analyze the impact of a material cybersecurity incident, as defined by the organization's appetite, on the organization (including the financial impact) as well as across the financial sector, as appropriate, per the organization's size, scope, complexity, and role in the financial sector. Describe how the process to determine materiality is integrated within the risk framework.

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.

DE.AE-5.1: The organization establishes and documents cyber event alert parameters and thresholds as well as rule-based triggers for an automated response within established parameters when known attack patterns, signatures or behaviors are detected.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

Once event logs with useful content have been identified, 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 and documents cyber event alert parameters and thresholds as well as rule-based triggers for an automated response within established parameters 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

Security Continuous Monitoring (DE.CM)

DE.CM-1.1: The organization establishes relevant system logging policies that include the types of logs to be maintained and their retention periods.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Information captured in logs is critical to detecting malicious activity and providing incident responders with crucial evidence for investigations. The organization should be thoughtful about the types of data included in logs throughout the organizations and should maintain formalized policies and procedures for logging and data retention.

Describe how the organization has established relevant event logging policies that include the types of logs to be maintained, data elements within logs, how they are correlated, and their retention periods.

Examples of Effective Evidence

- Event logging and monitoring policy, standard, and procedure
- Data retention policy and retention practices
- Use case examples (e.g., infrastructure, database, access, application, etc.)
- Examples of how event logs are reviewed and retained in a secure manner
- Documentation of the monitoring of logs
- Related reporting
- Proof of annual or more frequent independent reviews of logging practices to ensure appropriate log management (e.g., access controls, retention, and maintenance).

DE.CM-1.2: The organization implements systematic and real-time logging, monitoring, detecting, and alerting measures across multiple layers of the organization's infrastructure (covering physical perimeters, network, operating systems, applications and data).

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, monitoring, detecting, and alerting measures across multiple layers of the organization's infrastructure that produce actionable information. 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.CM-1.3: The organization deploys an 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 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

- 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-1.4: The organization implements mechanisms, such as alerting and filtering sudden high volume and suspicious incoming traffic, to prevent (Distributed) Denial of Services (DoS/DDoS) 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 prevent DoS/DDoS 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-2.1: The organization's controls include monitoring and detection of anomalous activities and potential cybersecurity events across the organization's physical environment and infrastructure, including unauthorized physical access to high-risk or confidential systems.

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 cybersecurity events across the organization's physical environment and infrastructure, including unauthorized physical access to high-risk or confidential systems.

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-3.1: 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, and software 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.

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

DE.CM-3.2: The organization performs logging and reviewing of the systems activities of privileged users, and monitoring for anomalies 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. Provide information regarding the review of system activities of privileged users and how monitoring for anomalies is implemented.

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-3.3: The organization conducts periodic cyber-attack simulations to detect control gaps in employee behavior, policies, procedures and resources.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Describe how the organization conducts periodic cyber-attack simulations to detect control gaps in employee behavior, policies, procedures, and resources. Cyber-attack simulations may include tabletop exercises, phishing exercises, penetration testing, red teaming, etc. Provide information on the frequency, scope, and the internal groups involved in simulations.

Examples of Effective Evidence

- Vulnerability management security policies, standards, and procedures
- Cyber threat analysis and reporting
- Security testing standards for applications and supporting infrastructure
- Related reporting (e.g., tabletop lessons learned)

DE.CM-4.1: The organization implements and manages appropriate tools to detect and block malware from infecting networks and systems.

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 implementation and management of tools to detect and block malware from infecting networks and systems. Provide information on malware protection and intrusion protection.

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

DE.CM-4.2: The organization implements email protection mechanisms to automatically scan, detect, and protect from any attached malware or malicious links present in the email.

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. As such, the organization should implement email protection mechanisms to protect the organization from malware or viruses.

Describe which email protection mechanisms have been implemented to automatically scan, detect, and protect from any attached malware or malicious links presented in email. 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

DE.CM-5.1: The organization implements safeguards against mobile malware and attacks for mobile devices connecting to corporate network and accessing corporate data (e.g., anti-virus, timely patch deployment, etc.).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Unmanaged mobile devices with access to confidential information can pose a significant risk. The organization should ensure that mobile devices with access to the organization's network and corporate data receive anti-virus and critical software patches from a centralized organization-managed system. The organization should also implement safeguards related to bring your own device (BYOD) for connecting to the corporate network.

Describe which safeguards the organization has implemented against mobile malware and attacks for mobile devices connecting to the corporate network and accessing corporate data. Provide information on the tools and processes such as anti-virus, patch deployment, and other.

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.

DE.CM-6.1: The organization authorizes and monitors all third-party connections.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization should control and monitor all third-party connections (e.g., cloud service providers, application programming interfaces (APIs), etc.). 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 authorizes and monitors all third-party connections. Provide information regarding the process.

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

DE.CM-6.2: The organization collaborates with third-party service providers to maintain and improve the security of external connections.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Describe how the organization collaborates with third-party service providers (e.g., core processing, online and mobile banking, settlement activities, disaster recovery services, cloud service providers) to maintain and improve the security of external connections, through application programming interfaces (APIs) or otherwise. 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

DE.CM-6.3: 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 the service provider's systems. 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

DE.CM-7.1: The organization implements appropriate controls to prevent use of unsupported and unauthorized software.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Unsupported operating systems and components 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 controls have been implemented to prevent the use of unsupported and unauthorized software. Provide information on the software management process.

Examples of Effective Evidence

- Unsupported and unauthorized software identification/review process and reports
- Related policies, standards, and procedures
- Proof that related tools for preventing, monitoring, and remediating of unauthorized software are in place
- Supported software
- Documentation that programs that can override system, object, network, virtual machine and application controls are restricted

DE.CM-7.2: The organization has policies, procedures and adequate tools in place to monitor, detect, and block access from/to devices, 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, connections, and data transfers. Provide information on the approved policies and procedures. Provide information on how the various tools achieve the requirement.

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-7.3: The organization sets up automatic and real-time alerts when an unauthorized software, hardware or configuration change occurs.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

The organization should have a comprehensive system for monitoring access to systems, devices, components, and software for unauthorized changes. The organization should set up automated processes or tools that can detect and prevent changes to hardware or software and can alert security staff when certain changes are attempted or executed.

Describe what the organization has in place for automatic and real-time alerts when an unauthorized software, hardware or configuration change occurs. Provide information on the use of privileged accounts with access to hardware and software configuration. Provide information on the use of security information and event management (SIEM) tooling, if applicable.

Examples of Effective Evidence

- Secure use of removable storage devices policies, standards, and procedures
- Storage security policies, standards, and procedures
- Mobile device security policies, standards, and procedures
- Security event logging and monitoring policies, standards, and procedures
- Privilege account policies, standards, and procedures
- Documents showing related tools for preventing, monitoring, and remediating unauthorized software, hardware or configuration changes are in place
- Proof that mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks
- Proof of related reporting

DE.CM-7.4: The organization implements web-filtering tools and technology to block access to inappropriate or malicious websites.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Describe the web-filtering tools and technology implemented to block access to inappropriate or malicious websites. Provide information on tools used.

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)

DE.CM-8.1: The organization conducts periodic vulnerability scanning, including automated scanning across all environments, to identify potential system vulnerabilities including publicly known vulnerabilities, upgrade opportunities, and new defense layers.

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. The vulnerability management process should include vulnerability scanning of all systems and applications on a routine basis based on the risk profile of the organization.

Describe how the organization conducts periodic vulnerability scanning, including automated scanning across all environments, to identify potential system vulnerabilities including publicly known vulnerabilities, upgrade opportunities, and new defense layers. Provide information on strategy and scope. Provide information regarding the tools utilized.

Examples of Effective Evidence

- Applications and supporting infrastructure security testing policies, standards, and procedures
- Vulnerability management security policies, standards, and procedures
- Baseline documentation
- Risk scoring on vulnerabilities
- Related tools
- Related reporting
- Proof that independent vulnerability scanning is conducted according to the risk assessment for the internal network
- Proof that vulnerability scans are utilized to provide insight into the effectiveness of the patch management process

DE.CM-8.2: The organization conducts, either by itself or by an independent third party, periodic penetration testing and red team testing on the organization's network, internet-facing applications or systems, and critical applications 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.

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 organization's network, 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

Detection Processes (DE.DP)

DE.DP-1.1: The organization has established and assigned roles and responsibilities for systematic monitoring and reporting processes.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

Appropriate staff should be responsible for monitoring and reporting suspicious activity. The organization's management should define the responsibility and authority of security personnel and system administrators that perform monitoring and reporting.

Describe the assigned roles and responsibility in place for systematic monitoring and 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

DE.DP-2.1: The organization's monitoring and detection processes comply with all applicable requirements.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Describe how the organization's monitoring and detection processes comply with all applicable requirements, including organizational requirements, legal and regulatory requirements, and industry standards.

Examples of Effective Evidence

- Security event logging and monitoring policies, standards, and procedures
- Access request and review security policies, standards, and procedures
- Logging and monitoring policies, standards, and procedures
- Escalation procedures
- Use cases
- Related reporting of key risk indicators (KRIs) and key performance indicators (KPIs)

DE.DP-3.1: The organization establishes a comprehensive testing program to conduct periodic and proactive testing and validation of the effectiveness of the organization's incident detection processes and controls.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Incident detection processes should be tested to validate the effectiveness of incident detection processes and controls through various exercises that emulate the types of events they are designed to detect. Incident detection processes may include the following design considerations: fault tolerance, adaptability, autonomy, and transparency, among others.

Describe the established and comprehensive incident detection processes and controls testing program in place. Provide information on the periodic and proactive testing and validation of the effectiveness of the organization's incident detection processes and controls.

Examples of Effective Evidence

- Proof of security testing for applications and supporting infrastructure policies, standards, and procedures
- Vulnerability management policies, standards, and procedures
- Related testing documentation (e.g., detection method reviews, red team or third-party testing, etc.)
- Use cases
- Remediation plans
- Test plans for business continuity/disaster recovery and incident response
- Proof of related reporting

DE.DP-4.1: The organization has established processes and protocols to communicate, alert and periodically report detected potential cyber-attacks and incident information including its corresponding analysis and cyber threat intelligence to 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 protocols to communicate, alert and periodically report detected potential cyber-attacks and incident information including its corresponding analysis and cyber threat intelligence to 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.DP-4.2: The organization tests and validates the effectiveness of the incident 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 reporting and communication processes to ensure that controls in place are effective.

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

DE.DP-5.1: The organization establishes a systematic and comprehensive program to periodically evaluate and improve the monitoring and detection processes and controls, as well as incorporate the lessons learned, as the threat landscape evolves.

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 established systematic and comprehensive program utilized to periodically evaluate and improve the monitoring and detection processes and controls. Describe how lessons learned are incorporated as the threat landscape evolves. Provide information on the linkage to the overall risk 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

RESPOND

Response Planning (RS.RP)

RS.RP-1.1: The organization's response plans are in place and executed during or after an incident.

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.

Describe how the organization's response plans are in place and executed during or after an incident. Provide information on the structure and process.

Refer to RS.IM-1.1 through RS.IM-2.1 for 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

Communications (RS.CO)

RS.CO-1.1: The organization's incident response plan contains clearly defined roles, responsibilities and levels of decision-making authority.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Describe how the organization's incident response plan contains 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. The organization's incident response 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.

RS.CO-1.2: The organization ensures cyber threat intelligence is made available to appropriate 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 cyber threat intelligence, which may include cyber incident information as appropriate, is made available to appropriate 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-1.3: The organization's personnel know their roles and responsibilities and order of operations when a response is needed.

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 order of operations 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

RS.CO-2.1: The organization's incident response plan describes how to appropriately document and report cyber events and related incident response activities.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The incident response team 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 describes how to appropriately document and report cyber events and related incident response activities. Security investigations, forensic analysis, and remediation are performed by qualified staff or third parties. Focus on the plan sections that relate to the documentation and reporting of cyber events and related incident response activities.

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

RS.CO-2.2: In the event of a cybersecurity incident, the organization notifies appropriate stakeholders including, as required, government bodies, self-regulatory agencies or any other supervisory bodies.

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 appropriate stakeholders including, as required, government bodies, self-regulatory agencies or any other supervisory bodies in the event of a cybersecurity incident. Provide information with a focus on stakeholders.

Examples of Effective Evidence

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

RS.CO-2.3: The organization's incident response program includes effective 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.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

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, other incident response teams, and system owners, among others.

Describe how the organization's incident response program includes effective 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-2.4: The organization's reporting requirements and capabilities are consistent with information-sharing arrangements within the organization's communities and the financial sector.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

An organization can establish information-sharing arrangements directly with peers and through industry information sharing organizations, such as FSSCC, FS-ISAC, industry associations, etc. Describe how the organization's reporting requirements and capabilities are consistent with information-sharing arrangements within the organization's communities and the financial sector.

Examples of Effective Evidence

- Security incident response policies, standards, and procedures
- Incident response examples or playbooks
- Related notification procedures
- Cyber threat/incident reporting examples
- Information sharing agreements, if applicable

RS.CO-3.1: Information is shared consistent with response plans.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The incident response program should include incident reporting procedures.

Describe how information is shared consistent with response plans. Provide information relating to the issuance of internal and external communications based upon the incident or threat severity level.

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

RS.CO-3.2: In the event of a cybersecurity incident, the organization shares information in an appropriate manner that could facilitate the detection, response, resumption, and recovery of its own systems and those of other financial sector participants through trusted channels.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Proactively sharing threat intelligence helps organizations achieve broader cybersecurity situational awareness among external stakeholders. As noted in RS.CO-2.4, an organization can establish threat intelligence sharing relationships directly with peers and through industry information sharing organizations, such as FS-ISAC, industry association, etc.

Describe how the organization shares information in an appropriate manner through trusted channels. Provide information related to the facilitation of detection, response, resumption, and recovery of internal systems and those of other financial sector participants.

Examples of Effective Evidence

- Security incident response policies, standards, and procedures
- Incident response examples or playbooks
- List of information sharing partners and agreements, if applicable
- Related notification procedures
- Cyber threat/incident information sharing examples

RS.CO-4.1: The organization has a plan to coordinate and communicate with internal and external stakeholders during or following a cyber-attack, as appropriate.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

The organization should have policies and procedures for communicating cyber incidents to internal and external stakeholders. Internal communication may occur through various methods, including designated privacy, legal, or corporate communications groups, among others.

Describe the organization's plan to coordinate and communicate with internal and external stakeholders during or following a cyber-attack as appropriate. Provide information on the communications plan activities.

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

RS.CO-5.1: The organization actively participates in multilateral information-sharing arrangements to facilitate a sector-wide response to large-scale incidents.

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.

Examples of Effective Evidence

- Security incident response policies, standards, and procedures
- Incident response examples or playbooks
- List of information sharing partners and agreements, if applicable
- Related notification procedures
- Cyber threat/incident information sharing examples

RS.CO-5.2: 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.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

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.

Examples of Effective Evidence

- Security incident response policies, standards, and procedures
- Cyber threat and resilience information sharing examples

RS.CO-5.3: The organization maintains ongoing situational awareness of its operational status and cybersecurity posture to pre-empt cyber events and respond rapidly to them.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

Describe the ongoing situational awareness of the organization's operational status and cybersecurity posture to pre-empt cyber events and respond rapidly to them. A proactive cyber risk management approach involves developing threat intelligence capabilities based on data collection and methods. The organization may use detection solutions and logging to identify and alert to unauthorized activity. Provide information on monitoring activities. Include information on red team and cybersecurity operation center functions and roles within.

Examples of Effective Evidence

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

Analysis (RS.AN)

RS.AN-1.1: Tools and processes are in place to ensure timely detection, alert, and activation of the incident response program.

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.). Describe the tools and processes that are in place to ensure timely detection, alert, and activation of the incident response program.

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 tools
- Use cases
- Logging and reporting examples
- Related assessment reporting

RS.AN-2.1: The organization uses cyber-attack scenarios to determine potential impact to critical business processes.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Describe how the organization uses cyber-attack scenarios to determine potential impact to critical 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.

Examples of Effective Evidence

- Security incident response policies, standards, and procedures
- Tabletop exercises and/or simulations
- Use cases
- Related assessment reporting

RS.AN-2.2: The organization performs a thorough investigation to determine the nature of a cyber-event, its extent, and the 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 of a cyber-event, its extent, and the 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. Describe how the organization collects and preserves data and evidence.

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-3.1: The organization has the capability to assist in or conduct forensic investigations of cybersecurity incidents and engineer protective and detective controls to facilitate the investigative process.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

Describe how the organization assists in or conducts forensic investigations of cybersecurity incidents, and engineers protective and detective controls to facilitate the investigative process. 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 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

RS.AN-4.1: The organization categorizes and prioritizes cybersecurity incident response consistent with response plans and criticality of systems 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. Describe 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.AN-5.1: The organization has established enterprise processes for receiving and appropriately channeling vulnerability disclosures from:

(1) Public sources (e.g., 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).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

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

RS.AN-5.2: 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 its severity and impact;

(4) Identifying affected stakeholders or customers; and

(5) Analyzing options to respond.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Describe how the organization has established enterprise processes to analyze disclosed vulnerabilities. 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

RS.AN-5.3: The organization has established processes to implement vulnerability mitigation plans, as well as validate their completion and effectiveness.

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. Provide information on how mitigation plans are reviewed and agreed upon. Provide information on how remediation is tested and verified.

Examples of Effective Evidence

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

Mitigation (RS.MI)

RS.MI-1.1: The organization contains cybersecurity incidents in a timely manner.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization's incident response plan should include procedures to contain and control an incident within defined parameters. The primary purpose of the containment phase is to limit and prevent further damage.

Describe how the organization contains cybersecurity incidents in a timely manner. Provide information on response plans and related response times. Describe controls for incident data collection and preservation.

Examples of Effective Evidence

- Incident response policies and procedures, including defined parameters for containing an incident
- Related incident response plans
- Priority response matrix

RS.MI-1.2: The organization's procedures include containment strategies and notifying potentially impacted third parties, as appropriate.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization's incident response plan should identify containment strategies for various types of incidents that might impact the organization's systems and/or information. Types of incidents may include unauthorized access to systems and information, DoS, malicious code injections, unauthorized use of system resources, unauthorized system scans and attempted access, ransomware, social engineering attempts, and spear phishing. Containment strategies vary based on the type of incident.

Describe how the organization's procedures include containment strategies. Additionally, the incident response plan should address how and when third-party vendors are notified if the compromise affects their system. Provide information on the process of notifying potentially impacted third parties as appropriate.

Examples of Effective Evidence

- Security incident response policies, standards, and procedures
- Incident response examples or playbooks
- Regulator notification procedures
- Data breach summary documents
- Notification examples
- Information sharing examples

RS.MI-2.1: The organization mitigates cybersecurity incidents in a timely manner.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Organizations should have the people, processes, and technology in place to safeguard critical assets and services. Incident response plans should outline the steps to mitigate an incident from preparation, detection and analysis, containment, eradication, and recovery.

Describe how the organization mitigates cybersecurity incidents in a timely manner. Provide examples.

Examples of Effective Evidence

- Security incident response policies, standards, and procedures
- Incident response examples and playbooks

RS.MI-3.1: The organization's incident response plan identifies requirements for the remediation of any identified weaknesses in systems and associated controls.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization should have procedures in place to restore system functionality once the infected devices have been restored or replaced. Describe how the organization's incident response plan identifies requirements for the remediation of any identified weaknesses in systems and associated controls. Include information regarding the related steps in the incident management plan and post incident reviews.

Examples of Effective Evidence

- Security incident response policies, standards, and procedures
- Incident response examples and playbooks

RS.MI-3.2: Vulnerabilities identified as a result of a cybersecurity incident are mitigated or documented by the organization as accepted risks and monitored.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

The organization should have procedures in place for restoring system functionality after identifying any vulnerabilities.

Describe how any vulnerabilities identified as a result of a cybersecurity incident are mitigated or documented by the organization as accepted risks and monitored.

Examples of Effective Evidence

- Remediation management documentation
- Vulnerability management security policy, standard, and procedures
- Mitigation management policy, standard, and procedures
- Risk acceptance policy, standard, and procedures

Improvements (RS.IM)

RS.IM-1.1: The organization's incident response plans are actively updated based on current cyber threat intelligence, information-sharing, and lessons learned following a cyber-event.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Organizations should stay current on cyber threat intelligence and proactively share threat intelligence to help achieve broader cybersecurity situational awareness and to ensure incident response plans are up to date. Describe how incident response plans are actively updated based on current cyber threat intelligence, information-sharing, and lessons learned following a cyber-event.

Examples of Effective Evidence

- Security incident response policies, standards, and procedures
- Incident response examples or playbooks
- Examples of updates to incident response plans

RS.IM-1.2: The results of the testing program are used by the organization to support ongoing improvement of its cyber resilience.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

The organization should periodically test systems and processes for their resilience and ability to recover from intrusions and attacks, as well as use the results from exercises to identify weaknesses in key controls, design, and the operating environment. Describe how the results of the testing program are used by the organization to support ongoing improvement of its cyber resilience. Provide information on the related organizational roles and responsibilities.

Examples of Effective Evidence

- Business continuity/resilience policy, standard, and procedure
- Testing metric reports
- Key observations reports
- Related testing result reports and briefs
- Documentation of results

RS.IM-1.3: The organization's cyber resilience and incident response programs have processes in place to incorporate lessons learned from cyber events that have occurred within and outside the organization.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

One of the most important parts of incident response is also the most often omitted: learning and improving. Holding a “lessons learned” meeting with all involved parties after an incident can be helpful in improving security measures and incident response. Provide information in support of the cyber resilience and incident response programs having processes in place to incorporate lessons learned from cyber events that have occurred within and outside the organization. Highlight the lessons learned processes associated with the cyber resilience and incident response programs.

Examples of Effective Evidence

- Security incident response policy, standard, and procedures
- Incident response examples or playbooks
- Business continuity/resilience policy, standard, and procedure
- Documentation of information-sharing or lessons learned exercises

RS.IM-2.1: The organization periodically reviews response strategy and exercises and updates them as necessary, based on:

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

(1) Lessons learned from cybersecurity incidents that have occurred (both within and outside 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; and

(5) New technological developments.

Response Guidance

Describe how the organization periodically reviews response strategy and exercises and updates them as necessary based on the five criteria within the statement (lessons learned, cyber threat intelligence, recent cyber-attacks, future cyber-attacks, 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

RECOVER

Recovery Planning (RC.RP)

RC.RP-1.1: 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

RC.RP-1.2: Organization's recovery plans are executed by first resuming critical services and core business functions, and without causing 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 without causing any potential concurrent and widespread interruptions to interconnected entities which may include 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-1.3: The recovery plan includes a minimum recovery time for the sector critical systems.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Demonstrate that the recovery plans include a minimum recovery time (also known as recovery time objective) for the sector critical systems. The organization should define recovery time objectives for critical systems, which are measured in terms of how long the business can survive following a disaster before operations are returned to normal.

Examples of Effective Evidence

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

RC.RP-1.4: The recovery plan includes recovery of clearing and settlement activities after a wide-scale disruption with the overall goal of completing material pending transactions on the scheduled settlement date.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Clearing and settlement organizations represent potential single points of failure in the financial system and therefore are crucial to the timely recovery and resumption of operations. Organizations could present systemic risk should they be unable to recover and resume critical clearing and settlement activities.

Demonstrate that the recovery plan includes the recovery of clearing and settlement activities after a wide-scale disruption with the overall goal of completing material pending transactions on the scheduled settlement date.

Examples of Effective Evidence

- Business continuity/resilience policy, standard, and procedures
- Data center recovery procedures
- Service continuity planning standards and procedures
- Related recovery procedures

RC.RP-1.5: The recovery plan includes recovery of resilience following a long-term loss of capability (e.g., site or 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 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

RC.RP-1.6: The recovery plan includes plans to come back for both traditional and highly available (e.g., cloud) infrastructure.

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 both traditional and highly available infrastructure 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 plans to come back for both traditional and highly available (e.g., cloud) infrastructure.

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

Improvements (RC.IM)

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

RC.IM-1.1: The organization refines its cyber resilience and incident response plans by actively identifying and incorporating crucial lessons learned from:

(1) Cybersecurity incidents that have occurred within the organization;

(2) Cybersecurity assessments and testing performed internally; and

(3) Widely reported events, industry reports and cybersecurity incidents that have occurred outside the organization.

Response Guidance

Describe how cyber resilience and incident response plans are refined by actively identifying and incorporating crucial lessons learned from the three identified criteria. The second criteria, cybersecurity assessments and testing performed internally, may include tabletop or lessons learned exercises. The organization should provide evidence of refinements to cyber resilience and incident response plans, such as documentation of tabletop or lessons learned exercises or other related examples.

Examples of Effective Evidence

- Security incident response policy, standard, and process
- System development and maintenance policy, standard, and procedures
- Incident response examples or playbooks
- Cyber threat intelligence and threat analysis report examples
- Documentation of tabletop or lessons learned exercises
- Related security assessments and reports

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

RC.IM-2.1: The organization periodically reviews recovery strategy and exercises and updates them as necessary, based on:

(1) Lessons learned from cybersecurity incidents that have occurred (both within and outside 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; and

(5) New technological developments.

Response Guidance

As noted in RC.IM-1.1 the organization refines and updates its cyber resilience and incident response plans. However, the organization should also periodically review its recovery strategy. Periodically reviewing the organization's recovery strategy, and exercising and updating the strategy as necessary, helps build confidence that resilience and recovery strategies meet business objectives. Describe how the recovery strategy and exercises are reviewed periodically and updated based on the five criteria within the Diagnostic Statement.

Examples of Effective Evidence

- Security incident response policy, standard, and procedures
- Business continuity/resilience policy, standard, and procedures
- Process diagrams
- Related strategy documents
- Related management reports and briefs
- Related threat intelligence reports

Communications (RC.CO)

RC.CO-1.1: The organization's governing body (e.g., the Board or one of its committees) ensures that a communication plan exists to notify internal and external stakeholders about an incident, as appropriate.

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 governing body should ensure that communication plans exist for notifying appropriate parties, including regulators, peer organizations, information sharing organizations.

Describe how the organization's governing body ensures that a communication plan exists to notify internal and external stakeholders about an incident, as appropriate. This includes a communication plan for interacting with the media, as needed.

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

RC.CO-1.2: The organization promptly communicates the status of recovery activities to regulatory authorities and relevant external stakeholders, as 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 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

RC.CO-2.1: Actionable and effective mitigation techniques are taken and communicated appropriately to restore and improve the organization's reputation after an incident.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Describe how actionable and effective mitigation techniques are taken and communicated appropriately to restore and improve the organization's reputation after an incident. Provide information on the stakeholders involved and the process.

Examples of Effective Evidence

- Regulator notification procedure
- Crisis response plan and procedure
- Media relations plan
- Related reporting and examples

RC.CO-3.1: The organization timely involves and communicates the recovery activities, procedures, cyber risk management issues to the appropriate governing body (e.g., the Board or one of its committees), senior management 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, 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

SUPPLY CHAIN / DEPENDENCY MANAGEMENT

Internal Dependencies (DM.ID)

DM.ID-1.1: The organization has integrated its internal dependency management strategy into the overall strategic risk management plan.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Response Guidance

Describe how the organization has integrated its internal dependency management strategy into the overall strategic risk management plan. Provide information on the integration of the internal dependency management strategy and the cyber risk management plan. Additionally, provide information on the overall risk management framework, including existing enterprise risk management, operational risk management, and supply chain risk management strategies.

Examples of Effective Evidence

- Enterprise risk management framework documentation
- Operational risk management framework documentation
- Cyber risk governance documentation
- Internal dependency management strategy

DM.ID-1.2: The organization monitors the effectiveness of its internal dependency management strategy.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Response Guidance

Describe how the organization monitors the effectiveness of its internal dependency management strategy. This may include periodic reviews of the strategy and any necessary updates to correspond to changes in the structure of the enterprise. The internal dependency management strategy can be integrated into existing enterprise risk management and operational risk management strategies by describing the roles and responsibilities that internal group support others during an incident or emergency. Provide information on how the framework is used along with roles and responsibilities of internal service providers.

Examples of Effective Evidence

- Enterprise risk management framework documentation
- Operational risk management framework documentation
- Internal dependency management strategy
- Internal dependency management reporting
- Metrics demonstrating monitoring of the internal dependency management strategy (e.g., key risk indicators, key performance indicators, etc.)
- Reporting structure

DM.ID-1.3: The organization ensures appropriate oversight of and compliance with the internal dependency management strategy implementation.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Response Guidance

Describe how the organization ensures appropriate oversight of and compliance with the internal dependency management strategy implementation. Often this is provided by inherent enterprise operational oversight, i.e., that all internal groups are effectively performing their respective functions within the enterprise. Provide information on the roles and responsibilities within the framework.

Examples of Effective Evidence

- Enterprise risk management framework documentation
- Operational risk management framework documentation
- Internal dependency governance policies, procedures, and reporting
- Reporting structure

DM.ID-1.4: The organization has established and applies appropriate controls to address the inherent risk of internal dependencies.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Response Guidance

Identification of dependencies and interdependencies among applications and services should be included when conducting information security assessments and testing. Describe the established and applied controls used to address the inherent risk of internal dependencies. Provide related risk framework information such as those found within existing enterprise risk management strategies or operational risk management strategies.

Examples of Effective Evidence

- Enterprise risk management framework documentation
- Operational risk management framework documentation
- Internal dependency management risk and control assessment examples

DM.ID-2.1: Roles and responsibilities for internal dependency management are defined and assigned.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Response Guidance

Various parts of the organization may be involved in internal dependency management (e.g., legal, IT, etc.). As a result, the organization's management should ensure that roles and responsibilities are clearly defined and assigned for all aspects of internal dependency management. Provide information on the roles and responsibilities for internal dependency management.

Examples of Effective Evidence

- Enterprise risk management framework documentation
- Operational risk management framework documentation
- Internal dependency management roles and responsibilities description
- Organizational chart
- Reporting structure

External Dependencies (DM.ED)

DM.ED-1.1: The organization has integrated its external dependency management strategy into the overall cyber risk management plan.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Describe how the organization has integrated its external dependency management strategy into the overall cyber risk management plan. For example, the organization may include standard language to contracts with third-parties related to cyber risk.

Describe how the external dependency management strategy works in concert with the existing enterprise risk management strategy and/or operational risk management strategy.

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
- Examples of contracts with third parties

DM.ED-1.2: The organization monitors the effectiveness of its external dependency management strategy to reduce cyber risks associated with external dependencies.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Management should continuously review the external dependency strategy to determine if gaps exists and work towards self-improvement of the program.

Describe how the organization monitors the effectiveness of its external dependency management strategy to reduce cyber risks associated with external dependencies.

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 external dependency management strategy
- Documentation showing resiliency testing in conjunction with external suppliers

DM.ED-1.3: The organization ensures appropriate oversight and compliance with the external dependency strategy implementation.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

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 external dependency 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
- External dependency management governance roles and responsibilities
- Due diligence policy, requirement, or questionnaire
- Other related third-party assessment processes, examples, and reporting

DM.ED-2.1: The organization has established policies, plans, and procedures to identify and manage cyber risks associated with external dependencies throughout those dependencies' lifecycles in a timely manner, including sector-critical systems and operations.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization's policies, plans, and procedures should include processes for inventorying critical third-parties and identifying and assessing cyber risks to external dependencies with those third parties.

Provide information on the established policies, plans, and procedures used to identify and manage cyber risks associated with external dependencies throughout those dependencies' 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 a security questionnaire, 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
- Security questionnaire
- Contractual language on security requirements (security schedule)
- Business impact analysis

DM.ED-2.2: The organization's dependency management policies, plans, and procedures are regularly updated.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization should establish a formal process that triggers review of the organization's dependency management program to determine if gaps exist and update policies, plans, and procedures to work towards self-improvement of the program.

Provide information related to the regular update of dependency management policies, plans, and procedures.

Examples of Effective Evidence

- Dependency management policy, standards, and procedures
- Third-party security policy, standard, and procedures
- Third-party risk management program
- Evidence of review of dependency management program
- Examples of updates to policies, plans, and procedures

DM.ED-2.3: The organization's dependency management policies, plans, and procedures have been reviewed and approved by appropriate organizational stakeholders.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Provide information supporting the organization's dependency management policies, plans, and procedures have been reviewed and approved by appropriate organizational stakeholders (e.g., Board, senior leadership, etc.). For example, policies may include a page indicating when it was last updated and who reviewed it.

Examples of Effective Evidence

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

DM.ED-2.4: Dependency management processes may allow the organization to adopt the security program(s) of its "affiliate(s)" as long as such program provides an appropriate level of control and assurance.

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.

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

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Third-party security review methodology
- Third-party risk assessment program
- Related reporting and examples

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

DM.ED-2.5: The organization's dependency management process identifies third-party relationships that are in place, including those relationships that were established without formal approval.

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 dependency management process identifies 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 third-party vendors. 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

DM.ED-3.1: Roles and responsibilities for external dependency management are defined and assigned.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Various parts of the organization may be involved in external dependency management (e.g., legal, IT, etc.). As a result, the organization's management should ensure that roles and responsibilities are clearly defined and assigned for all aspects of external dependency management, including initiation of the relationship, ongoing oversight, and termination. Provide information on the roles and responsibilities for external dependency management.

Examples of Effective Evidence

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Documentation of roles and responsibilities for external dependencies
- Related reporting and examples

DM.ED-3.2: Responsibilities for ongoing independent oversight (external) of third-party access are defined and assigned.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	

Response Guidance

A third-party security policy or vendor management policy may assign specific responsibility to manage and/or provide ongoing oversight of third-party access to the organization's network. Describe how responsibilities for ongoing independent oversight of third-party access are defined and assigned by the organization.

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

DM.ED-4.1: The organization ensures that cyber risks associated with external dependencies are consistent with cyber risk appetite approved by an appropriate governing body (e.g., the Board or one of its committees).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Third-parties that can affect the risk profile of the organization include those with access to internal systems or nonpublic customer information, those storing and/or processing information that support critical activities, and cloud computing providers that support control activities.

Describe how the organization ensures that cyber risks associated with external dependencies are consistent with cyber risk appetite approved by an appropriate governing body (e.g., the Board or one of its committees). Describe the analysis or process to determine the level of risk a third-party poses to the organization and the comparison to the risk appetite statement.

Examples of Effective Evidence

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Third-party security review methodology
- Third-party risk assessment
- Risk appetite statements
- Business impact analysis

DM.ED-4.2: The organization has established and applies appropriate policies and controls to address the inherent risk of external dependencies to the enterprise and the sector, if appropriate.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

Describe how the organization has established and applies appropriate policies and controls to address the risk of external dependencies to the enterprise and the sector, if appropriate. Third-parties that can affect the risk profile of the organization include those with access to internal systems or nonpublic customer information, those storing and/or processing information that support critical activities, and cloud computing providers that support control activities.

Examples of Effective Evidence

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Third-party risk assessments
- Business impact analysis

DM.ED-4.3: The organization conducts a risk assessment to define appropriate controls to address the cyber risk presented by each external partner, implements these controls, and monitors their status throughout the lifecycle of partner relationships.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Outsourced relationships have the potential of introducing new or expanded cybersecurity risks. The organization should review the list of all third-party service providers to determine criticality (e.g., high, medium, low risk or critical, non-critical, etc.) and conduct a risk assessment to determine the appropriate controls.

Provide information on how the organization conducts a risk assessment to define appropriate controls to address the cyber risk presented by each external partner, implements these controls, and monitors their status throughout the lifecycle of partner relationships. Provide documentation of any actions taken to mitigate risk.

Examples of Effective Evidence

- Third-party security policy, standard, and procedures
- Third-party risk management program
- Third-party security review methodology
- Third-party risk assessments
- Documentation of risk assessment outputs and any actions taken to mitigate risk
- Related reporting and examples

DM.ED-4.4: The organization has a documented third-party termination/exit strategy to include procedures for timely removal of the third-party access when no longer required.

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 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 when no longer required.

Refer to DM.ED-4.5 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 exit clauses
- Related reporting and examples

DM.ED-4.5: 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 vendor replacements 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 vendor out of business or severely impact delivery of services to the organization, sector-critical systems, or the 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

DM.ED-5.1: The organization has identified and monitors the organizational ecosystem of external dependencies for assets/systems that are critical to the enterprise and the financial services sector.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Response Guidance

Within the listing of external dependencies (refer to DM.ED-5.2), the organization identifies the external dependencies based on their criticality to the business functions they support, the organization's mission, and the financial sector.

Describe how the organization identifies and monitors the organizational ecosystem of external dependencies for assets/systems that are critical to both the enterprise and the financial services sector. Appropriate controls and monitoring should be in place between the organization and external dependencies. Controls may include intrusion detection systems, intrusion prevention systems, and SIEM tools. Ongoing review of vendors occurs on a flow basis, based on risk, to ensure all critical vendors obtain periodic due diligence reviews.

Examples of Effective Evidence

- Inventory of critical external dependencies and business functions
- Identification criteria of critical external dependencies and related business functions
- Due diligence reviews or evidence of other monitoring processes
- Third-party security policy, standard, and procedures
- Third-party risk management program
- Third-party security review methodology

DM.ED-5.2: The organization maintains a current, accurate, and complete listing of all external dependencies and business functions, including mappings to supported assets and business functions.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

A key aspect of external dependency management is having the ability to monitor all external dependencies and trusted connections that support an organization's cyber risk management strategy. Describe how the organization maintains a current, accurate, and complete listing of all external dependencies and their business functions, including identification criteria used for determining external dependencies and business functions within the organization. The listing should include mappings to supported assets and business functions. Organizations may use a data flow diagram or diagram of external vendor connections to show mappings and information flowing in and out of the organization's network. A cloud register should be maintained to document the records related to regulatory requirements that are held by a cloud provider. This register should be maintained throughout the period in which the records are required to be kept by law or regulation.

Within the listing, the organization may designate external dependencies by criticality. Refer to DM.ED-5.1 for more information on identifying and monitoring critical external dependencies.

Examples of Effective Evidence

- Inventory/listing of external dependencies and business functions
- Identification criteria of external dependencies and related business functions
- Mappings, data flow diagrams, or other network diagrams of external vendors connectivity or connections
- Third-party security policy, standard, and procedures
- Third-party risk management program
- Third-party connection authorizations

DM.ED-5.3: The organization has prioritized functions, activities, products, and services provided by external dependencies based on criticality.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

The organization should prioritize external dependencies (as identified in DM.ED-5.1) based on their criticality to the business functions they support, the organization's mission, and the financial sector. The organization should define critical services associated with external connectivity and reflect criticality in a network diagram or topology.

Describe how the organization has prioritized functions, activities, products, and services provided by external dependencies based on criticality.

Examples of Effective Evidence

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

DM.ED-5.4: The organization has prioritized 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

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 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

DM.ED-6.1: The organization has documented minimum cybersecurity requirements for critical third parties that, at a minimum, meet cybersecurity practices of the organization.

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 critical third parties should be required to follow minimum cybersecurity requirements that meet the cybersecurity practices of the organization. These requirements may be documented within service contracts, Requests for Proposals (RFP), and/or other reporting.

Describe the documented minimum cybersecurity requirements for critical third parties that, at a minimum, meet cybersecurity practices of the organization.

Examples of Effective Evidence

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

CYBER RISK INSTITUTE

DM.ED-6.2: The organization's contracts require third parties to implement minimum cybersecurity requirements and to maintain those practices for the life of the relationship.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

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.

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. Third parties may need to maintain cybersecurity requirements after the relationship ends. 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

DM.ED-6.3: Minimum cybersecurity requirements for third parties include how the organization will monitor security of its external dependencies to ensure that requirements are continually satisfied.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

As referenced in DM.ED-6.1 and DM.ED-6.2, the organization has documented minimum cybersecurity requirements for third parties. These minimum cybersecurity requirements should include language and details on how the organization will monitor third parties to ensure compliance with requirements.

Describe how minimum cybersecurity requirements for third parties, identified in DM.ED-6.1, as outlined in contracts or other documentation, include how the organization will monitor security of external dependencies to ensure that requirements are continually satisfied.

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

DM.ED-6.4: Minimum cybersecurity requirements for third parties include consideration of whether the third party is responsible for the security of the organization's confidential data and of geographic limits on where data can be stored and transmitted.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

As referenced in DM.ED-6.1 and DM.ED-6.2, the organization has documented minimum cybersecurity requirements for third parties. Describe how the minimum cybersecurity requirements for third parties include consideration of whether the third party is responsible for the security of the organization's confidential data and of geographic limits on where data can be stored and transmitted. The organization should be aware of and approve where customer data is being processed and/or stored by third parties. Contracts should specifically define where this will take place.

In outsourcing to cloud service providers, the organization should consider the data classification, data segregation, and recoverability. Contracts and service level agreements with cloud service providers should be specific as to the ownership, location and format of the data, and dispute resolution.

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
- Related third-party reporting

DM.ED-6.5: Minimum cybersecurity requirements for third parties include how the organization and its suppliers and partners 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 cybersecurity incident;

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 potential impact of a cyber-event into their BCP process and ensure appropriate resilience capabilities are in place.

Response Guidance

As referenced in DM.ED-6.1 and DM.ED-6.2, the organization has documented minimum cybersecurity requirements for third parties. Describe how minimum cybersecurity requirements for 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

DM.ED-6.6: Minimum cybersecurity requirements for third parties identify conditions of and the recourse available to the organization should the third party fail to meet their cybersecurity requirements.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

As referenced in DM.ED-6.1 and DM.ED-6.2, the organization has documented minimum cybersecurity requirements for third parties. Describe how the minimum cybersecurity requirements for third parties identify conditions of and the recourse available to the organization should the third party fail to meet their cybersecurity requirements. 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

DM.ED-6.7: Minimum cybersecurity requirements for third parties cover the entire relationship lifecycle, including return or destruction of data during cloud or virtualization use and upon relationship termination.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

As referenced in DM.ED-6.1 and DM.ED-6.2, 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 during cloud or virtualization use and upon relationship termination. 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

DM.ED-7.1: The organization has a formal program for third-party due diligence and monitoring.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization should conduct appropriate due diligence on all potential third parties before selecting and entering into contracts or relationships with third parties and should establish formal processes for monitoring third parties. Describe the organization's formal program for third-party due diligence and monitoring.

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

DM.ED-7.2: The organization conducts regular third-party reviews for critical vendors to validate that appropriate security controls have been implemented.

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 frequency and detailed level of review. 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 and the frequency of reviews. Describe how the organization conducts regular third-party reviews for critical vendors to validate that appropriate security controls have been implemented. 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

DM.ED-7.3: A process is in place to confirm that the organization's third-party service providers conduct due diligence of their own third parties (e.g., subcontractors).

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 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).

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

DM.ED-7.4: A process is in place to confirm that the organization's third-party service providers conduct periodic resiliency testing or justify why it is not needed.

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Response Guidance

The organization's third-party oversight should include reviewing third parties' resilience plans. The organization's management may also actively participate in third-party service provider testing programs. Provide information on the process in place and used to confirm that the organization's third-party service providers conduct periodic resiliency testing or justify why it is not needed.

Examples of Effective Evidence

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

Resilience (DM.RS)

DM.RS-1.1: The organization has an enterprise-wide cyber resilience (including business continuity, and incident response) strategy and program.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓	✓	✓

Response Guidance

The organization should have an enterprise-wide cyber resilience strategy and program because cyber 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 cyber resilience strategy should be incorporated into the overall business strategy and risk management of the organization. Describe the enterprise-wide cyber resilience (including business continuity and incident response) 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

DM.RS-1.2: The cyber resilience strategy and program are based on the organization's enterprise-wide cyber risk management strategy that addresses the risks that the organization may present to other critical infrastructure sectors and the risk that the organization may present to other firms in the financial sector.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Cyber threats and events 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 based on the organization's enterprise-wide cyber risk management strategy. Describe how the strategy and program addresses 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

DM.RS-1.3: The cyber resilience program ensures that the organization can continue operating critical business functions and deliver services to stakeholders during cybersecurity incidents and cyber-attacks (e.g., propagation of malware or corrupted data).

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

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

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

DM.RS-2.1: The organization has incorporated its external dependencies and critical business partners into its cyber resilience (e.g., incident response, business continuity, and disaster recovery) strategy, plans, and exercises.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

The organization's external dependency management strategy should be incorporated into the cyber resilience strategy. Describe how the organization has incorporated its external dependencies and critical business partners into its cyber resilience (e.g., incident response, business continuity, and disaster recovery) strategy, plans, 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

DM.RS-2.2: The organization's cyber resilience strategy addresses the organization's obligations for performing core business functions including those performed for the financial sector as a whole, in the event of a disruption, including the potential for multiple concurrent or widespread interruptions and cyber-attacks on multiple elements of interconnected critical infrastructure, such as energy and telecommunications.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

For cyber-attacks that may potentially corrupt or destroy critical data, recovery strategies should be designed to achieve recovery point objectives based on the criticality of the data necessary to keep the organization operational. Describe how the organization's cyber resilience strategy addresses the organization's obligations for performing core business functions including those performed for the financial sector as a whole, in the event of a disruption. Describe how the potential for multiple concurrent or widespread interruptions and cyber-attacks on multiple elements of interconnected critical infrastructure, such as energy and telecommunications, are accounted for in the resilience strategy.

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
- Related response plan detail

DM.RS-2.3: The organization designs and tests its cyber resilience plans, and exercises to support financial sector's sector-wide resilience and address 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 cyber 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 designs and tests its cyber resilience plans, and exercises 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

DM.RS-2.4: The organization periodically identifies and tests alternative solutions in case an 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 cyber 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 an 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

DM.RS-2.5: When planning and executing incident response and recovery activities, the organization takes into consideration sector-wide impact of its systems and puts a priority on response and recovery activities for those systems ahead of the other systems.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

Organizations should consider how to prioritize the monitoring, incident response, and recovery of systems that are critical to the enterprise and financial sector. Describe how during the planning and executing incident response and recover activities, the organization takes into consideration sector-wide impact of its systems and puts a priority on response and recovery activities for those systems ahead of the other systems.

Examples of Effective Evidence

- Business continuity/resilience policy, standard, and procedures
- Business impact analysis documentation
- Security incident response policy, standard, and procedures
- Incident response examples or playbooks
- Related test summaries and reports

Business Environment (DM.BE)

DM.BE-1.1: The cyber risk strategy identifies and communicates the organization's role as it relates to other critical infrastructures and as a component of the financial services sector.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

The cyber risk management strategy should recognize the organization's role in the sector and as it relates to other critical infrastructures. Strategy documents should include information to demonstrate the organization's recognition of its role and impact on the financial services sector and other critical infrastructures. Describe how the cyber risk strategy identifies and communicates the organization's role as it relates to other critical infrastructures and as a component of the financial services sector.

Examples of Effective Evidence

- Cyber risk management strategy and framework
- Business continuity/resilience policy, standard, and procedures

DM.BE-1.2: A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across other sectors the institution depends upon.

TIER 1	TIER 2	TIER 3	TIER 4
✓	✓		

Response Guidance

The organization should have a formal process in place for the independent audit function, to be performed either by internal audit, an external third party, or both. Describe the formal process in place for the independent audit function to update the scope of the audit or evaluation based on changes to the evolving threat landscape across other sectors the organization depends upon. Provide information on the audit assessment process. For example, the financial sector is highly dependent on the energy and telecommunications sector. Cyber threats that target other sectors with high interdependence to financial services may warrant the organization investing more in power or communications resilience or additional controls to protect sensitive data. The independent audit function should update its procedures to adjust for these increased cyber threats and additional controls to mitigate them.

Examples of Effective Evidence

- Audit plans, including evidence of updates
- Scope documentation for specific audits or evaluations

DM.BE-2.1: 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

DM.BE-2.2: The organization has prioritized monitoring of systems 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. Describe how the organization has prioritized 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
- Tooling
- Related reporting and examples

DM.BE-3.1: Cyber resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).

TIER 1	TIER 2	TIER 3	TIER 4
✓			

Response Guidance

Describe the establishment of 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.

Examples of Effective Evidence

- Service continuity plans
- Inventory management reporting
- Critical services inventory and related dependencies

CYBER RISK INSTITUTE

APPENDIX A – ABBREVIATIONS

BYOD	Bring Your Own Device
CAT	Cybersecurity Assessment Tool
CCAR	Comprehensive Capital Analysis and Review
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technology
FFIEC	Federal Financial Institutions Examination Council
FSARC	Financial Systemic Analysis & Resilience Center
FS-ISAC	Financial Services Information Sharing and Analysis Center
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
IIoT	Industrial internet of things
IoT	Internet of things
ISO	International Organization for Standardization
IT	Information Technology
KCI	Key Control Indicator
KPI	Key Performance Indicator
KRI	Key Risk Indicator
NIST	National Institute of Standards and Technology
PCI-DSS	Payment Card Industry Data Security Standard
SDLC	System Development Life Cycle
SIEM	Security Information and Event Management

CYBER RISK INSTITUTE

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	
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	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.

	strategy for mission assurance, business assurance, or operational resilience.	
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.	
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	refers to allowing only authorized access for users which are necessary to accomplish the assigned tasks in accordance with organizational missions and business functions	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	
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 third party to whom a financial institution outsources activities that the institution 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.SF-1.1	The organization has a cyber risk management strategy and framework that is approved by the appropriate 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.SF-1.2	An appropriate governing authority (e.g., the Board or one of its committees) oversees and holds senior management accountable for implementing the organization's cyber risk management strategy and framework.	1	2	3	4
GV.SF-1.3	The organization's cyber risk management strategy identifies and documents the organization's role as it relates to other critical infrastructures outside of the financial services sector and the risk that the organization may pose to them.	1	2		
GV.SF-1.4	The cyber risk management strategy identifies and communicates the organization's role within the financial services sector as a component of critical infrastructure in the financial services industry.	1	2		
GV.SF-1.5	The cyber risk management strategy and framework establishes and communicates priorities for organizational mission, objectives, and activities.	1	2	3	
GV.SF-2.1	The cyber risk management strategy and framework is appropriately informed by applicable international, national, and financial services industry standards and guidelines.	1	2	3	4
GV.SF-3.1	An appropriate governing authority (e.g., the Board or one of its committees) endorses and periodically reviews the cyber risk appetite and is regularly informed about the status of and material changes in the organization's inherent cyber risk profile.	1	2	3	
GV.SF-3.2	An appropriate governing authority (e.g., the Board or one of its committees) periodically reviews and evaluates the organization's ability to manage its cyber risks.	1	2	3	4
GV.SF-3.3	The cyber risk management framework provides mechanisms to determine the adequacy of resources to fulfill cybersecurity objectives.	1	2	3	
GV.SF-4.1	The risk appetite is informed by the organization's role in critical infrastructure.	1	2		
GV.RM-1.1	The cyber risk management program incorporates cyber risk identification, measurement, monitoring, and reporting.	1	2	3	4
GV.RM-1.2	The cyber risk management program is integrated into daily operations and is tailored to address enterprise-specific risks (both internal and external) and evaluate the organization's cybersecurity policies, procedures, processes, and controls.	1	2		
GV.RM-1.3	As a part of the cyber risk management program, the organization has documented its cyber risk assessment process and methodology, which are periodically updated to address changes to the risk profile and risk appetite (e.g., new technologies, products, services, interdependencies, and the evolving threat environment).	1	2	3	
GV.RM-1.4	The cyber risk assessment process is consistent with the organization's policies and procedures and includes criteria for the evaluation and categorization of enterprise-specific cyber risks and threats.	1	2	3	4
GV.RM-1.5	The cyber risk management program and risk assessment process produce actionable recommendations that the organization uses to select, design, prioritize, implement, maintain, evaluate, and modify security controls.	1	2	3	4
GV.RM-1.6	The cyber risk management program addresses identified cyber risks in one of the following ways: risk acceptance, risk mitigation, risk avoidance, or risk transfer, which includes cyber insurance.	1	2	3	4
GV.RM-2.1	The organization has established a cyber risk tolerance consistent with its risk appetite, and integrated it into technology or operational risk management, as appropriate.	1	2		
GV.RM-2.2	The cyber risk management strategy articulates how the organization intends to address its inherent cyber risk (before mitigating controls or other factors are taken into consideration).	1	2	3	
GV.RM-2.3	The cyber risk management strategy articulates how the organization would maintain an acceptable level of residual cyber risk set by the appropriate governing authority (e.g., the Board or one of its committees).	1	2	3	

GV.RM-3.1	The cyber risk management framework is integrated into the enterprise risk management framework.	1	2	3	
GV.RM-3.2	The organization has a process for monitoring its cyber risks including escalating those risks that exceed risk tolerance to management.	1	2		
GV.RM-3.3	The organization's cyber risk management framework provides for segregation of duties between policy development, implementation, and oversight to ensure rigorous review of both policy and implementation.	1	2		
GV.PL-1.1	The organization maintains a documented cybersecurity policy or policies approved by a designated Cybersecurity Officer (e.g., CISO) or an appropriate governing authority (e.g., the Board or one of its committees).	1	2	3	4
GV.PL-1.2	The organization's cybersecurity policy integrates with an appropriate employee accountability policy to ensure that all personnel are held accountable for complying with cybersecurity policies and procedures.	1	2	3	4
GV.PL-2.1	The cybersecurity policy is supported by the organization's risk management program.	1	2	3	4
GV.PL-2.2	Cybersecurity processes and procedures are established based on the cybersecurity policy.	1	2	3	4
GV.PL-2.3	The cybersecurity policy is periodically reviewed and revised under the leadership of a designated Cybersecurity Officer (e.g., CISO) to address changes in the risk profile and risk appetite (e.g., new technologies, products, services, interdependencies, and the evolving threat environment).	1	2	3	4
GV.PL-3.1	The cybersecurity policy, strategy and framework should take into account the organization's legal and regulatory obligations.	1	2	3	4
GV.PL-3.2	The organization's cybersecurity policies are consistent with its privacy and civil liberty obligations.	1	2	3	4
GV.PL-3.3	The organization implements and maintains a documented policy or policies that address customer data privacy, and 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.RR-1.1	The organization coordinates and aligns roles and responsibilities for personnel implementing, managing, and overseeing the effectiveness of the cybersecurity strategy and framework with internal and external partners.	1	2	3	
GV.RR-2.1	The organization has designated a 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-2.2	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-2.3	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.RR-2.4	The organization provides adequate resources to maintain and enhance the cybersecurity situational awareness of senior managers within the organization.	1	2	3	4
GV.SP-1.1	The organization has established, and maintains, a cybersecurity program designed to protect the confidentiality, integrity and availability of its information and operational systems, commensurate with the organization's risk appetite.	1	2	3	4
GV.SP-1.2	Based on a periodic risk assessment, the organization's cybersecurity program identifies and implements appropriate security controls to manage applicable cyber risks within the risk tolerance set by the governing authority (e.g., the Board or one of its committees).	1	2	3	
GV.SP-2.1	The organization implements a repeatable process to develop, collect, store, report, and refresh actionable cybersecurity key performance indicators and metrics.	1	2		
GV.SP-2.2	The organization develops, implements, and reports to management and the appropriate governing body (e.g., the Board or one of its committees) key cybersecurity performance indicators and metrics based on the cyber risk strategy and framework to measure, monitor, and report actionable indicators to help guide the security program.	1	2		

GV.SP-2.3	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		
GV.IR-1.1	The organization's enterprise-wide cyber risk management framework includes an independent risk management function that provides assurance that the cyber risk management framework is implemented as intended.	1	2		
GV.IR-1.2	An independent risk management function 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 cyber risk management framework.	1	2		
GV.IR-1.3	The independent risk management function has appropriate understanding of the organization's structure, cybersecurity program, and relevant risks and threats.	1	2		
GV.IR-1.4	Individuals responsible for independent risk management and oversight are independent of business line management, including senior leadership.	1	2		
GV.IR-2.1	An independent risk management function assesses the appropriateness of the cyber risk management program according to the organization's risk appetite.	1	2		
GV.IR-2.2	An independent risk management function frequently and recurrently assesses the organization's controls and cyber risk exposure, identifies opportunities for improvement based on assessment results, and proposes risk mitigation strategies and improvement actions when needed.	1	2		
GV.IR-3.1	An independent risk management function reports to the appropriate governing authority (e.g., the Board or one of its committees) and to the appropriate risk management officer within the organization on the implementation of the cyber risk management framework throughout the organization.	1	2		
GV.AU-1.1	The organization has an independent audit function.	1	2	3	4
GV.AU-1.2	The organization has an independent audit plan that provides for an evaluation of the organization's compliance with the appropriately approved cyber risk management framework and its cybersecurity policies and processes including how well the organization adapts to the evolving cyber risk environment while remaining within its stated risk appetite and tolerance.	1	2	3	
GV.AU-1.3	An independent audit function tests security controls and information security policies.	1	2	3	4
GV.AU-1.4	An independent audit function assesses compliance with applicable laws and regulations.	1	2	3	4
GV.AU-2.1	A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across the sector.	1	2	3	
GV.AU-2.2	A formal process is in place for the independent audit function to update its procedures based on changes to the organization's risk appetite and risk tolerance.	1	2		
GV.AU-3.1	An independent audit function reviews cybersecurity practices and identifies weaknesses and gaps.	1	2	3	4
GV.AU-3.2	An 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-3.3	An independent audit function reports to the appropriate 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 cyber risk tolerance has been exceeded in any part of the organization.	1	2	3	4
GV.TE-1.1	The organization identifies how cybersecurity will support emerging technologies that support business needs (e.g., cloud, mobile, IoT, IIoT, etc.) by integrating cybersecurity considerations into the lifecycle of new technologies from their inception.	1	2	3	4
GV.TE-1.2	The organization applies its cyber risk management framework to all technology projects.	1	2	3	4
GV.TE-2.1	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	
	IDENTIFY				
ID.AM-1.1	The organization maintains a current and complete asset inventory of physical devices, hardware, and information systems.	1	2	3	4
ID.AM-2.1	The organization maintains a current and complete inventory of software platforms and business applications.	1	2	3	4

ID.AM-3.1	The organization maintains an inventory of internal assets and business functions, that includes mapping to other assets, business functions, and information flows.	1	2		
ID.AM-3.2	The organization maintains a current and complete inventory of types of data being created, stored, or processed by its information assets.	1	2		
ID.AM-3.3	The organization's asset inventory includes maps of network resources, as well as connections with external and mobile resources.	1	2	3	4
ID.AM-4.1	The organization maintains an inventory of external information systems.	1	2	3	4
ID.AM-5.1	The organization implements and maintains a written risk-based policy or policies on data governance and classification, approved by a Senior Officer or the organization's governing body (e.g., the Board or one of its committees).	1	2	3	
ID.AM-5.2	The organization's resources (e.g., hardware, devices, data, and software) are prioritized for protection based on their sensitivity/classification, criticality, vulnerability, business value, and importance to the organization.	1	2	3	
ID.AM-6.1	Roles and responsibilities for the entire cybersecurity workforce and directly managed third-party personnel are established, well-defined and aligned with internal roles and responsibilities.	1	2	3	4
ID.RA-1.1	The organization's business units identify, assess and document applicable cyber risks and potential vulnerabilities associated with business assets to include workforce, data, technology, facilities, service, and IT connection points for the respective unit.	1	2	3	4
ID.RA-2.1	The organization participates actively (in geopolitical alignment with its business operations) in applicable 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		
ID.RA-3.1	The organization identifies, documents, and analyzes threats that are internal and external to the firm.	1	2	3	4
ID.RA-3.2	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		
ID.RA-3.3	The organization regularly reviews and updates results of its cyber threat analysis.	1	2	3	4
ID.RA-4.1	The organization's risk assessment approach includes identification of likelihood and potential business impact of applicable cyber risks being exploited.	1	2	3	4
ID.RA-5.1	Cyber threats, vulnerabilities, likelihoods, and impacts are used to determine overall cyber risk to the organization.	1	2	3	4
ID.RA-5.2	The organization considers threat intelligence received from the organization's participants, service and utility providers and other industry organizations.	1	2	3	
ID.RA-5.3	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			
ID.RA-5.4	The organization's business units assess, on an ongoing basis, the cyber risks associated with the activities of the business unit.	1	2		
ID.RA-5.5	The organization tracks connections among assets and cyber risk levels throughout the life cycles of the assets.	1			
ID.RA-5.6	The organization determines ways to aggregate cyber risk to assess the organization's residual cyber risk.	1	2		
ID.RA-6.1	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-6.2	Independent risk management is required to analyze cyber risk at the enterprise level to identify and ensure effective response to events with the potential to impact one or multiple operating units.	1	2		
	PROTECT				
PR.AC-1.1	Physical and logical access to systems is permitted only for individuals who have a legitimate business requirement and have been authorized.	1	2	3	4

PR.AC-1.2	User access authorization is limited to individuals who are appropriately trained and monitored.	1	2	3	4
PR.AC-1.3	Identities and credentials are actively managed or automated for authorized devices and users (e.g., removal of default and factory passwords, revocation of credentials for users who change roles or leave the organization, etc.).	1	2	3	
PR.AC-2.1	The organization manages and protects physical access to information assets (e.g., session lockout, physical control of server rooms).	1	2	3	4
PR.AC-3.1	Remote access is actively managed and restricted to necessary systems.	1	2	3	4
PR.AC-3.2	The organization implements multi-factor authentication, or at least equally secure access controls for remote access, if it is warranted by applicable risk considerations.	1	2	3	4
PR.AC-4.1	The organization limits access privileges to the minimum necessary.	1	2	3	4
PR.AC-4.2	The organization institutes strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements.	1	2	3	4
PR.AC-4.3	The organization institutes controls over service account (i.e., accounts used by systems to access other systems) lifecycles to ensure strict security over creation, use, and termination; access credentials (e.g., no embedded passwords in code); frequent reviews of account ownership; visibility for unauthorized use; and hardening against malicious insider use.	1	2	3	4
PR.AC-5.1	Networks and systems are segmented to maintain appropriate security.	1	2	3	4
PR.AC-5.2	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).	1	2	3	4
PR.AC-6.1	The organization authenticates identity and validates the authorization level of a user before granting access to its systems.	1	2	3	4
PR.AC-7.1	The organization performs a risk assessment for prospective users, devices and other assets which authenticate into its ecosystem with a specific focus on: (1) The type of data being accessed (e.g., customer PII, public data); (2) The risk of the transaction (e.g., internal-to-internal, external-to-internal); (3) The organization's level of trust for the accessing agent (e.g., external application, internal user); and (4) The potential for harm.	1			
PR.AC-7.2	Based on the risk level of a given transaction, the organization has defined and implemented authentication requirements, such as including implementing multi-factor, out-of-band authentication for high risk transactions.	1	2	3	4
PR.AT-1.1	All personnel (full-time or part-time; permanent, temporary or contract) receive periodic cybersecurity awareness training, as permitted by law.	1	2	3	4
PR.AT-1.2	Cybersecurity awareness training includes at a minimum appropriate awareness of and competencies for data protection, detecting and addressing cyber risks, and how to report any unusual activity or incidents.	1	2	3	4
PR.AT-1.3	Cybersecurity awareness training is updated on a regular basis to reflect risks identified by the organization in its risk assessment.	1	2	3	4
PR.AT-2.1	High-risk groups, such as those with privileged system access 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-2.2	Cybersecurity personnel receive training appropriate for their roles and responsibilities in cybersecurity, including situational awareness training sufficient to maintain current knowledge of cyber threats and countermeasures.	1	2	3	4
PR.AT-2.3	A mechanism is in place to verify that key cybersecurity personnel maintain current knowledge of changing cyber threats and countermeasures.	1	2	3	4
PR.AT-3.1	The organization has established and maintains a cybersecurity awareness program through which the organization's customers are kept aware of their role in cybersecurity, as appropriate.	1	2	3	4
PR.AT-3.2	Cybersecurity training provided through a third-party service provider or affiliate should be consistent with the organization's cybersecurity policy and program.	1	2	3	4

PR.AT-3.3	Cybersecurity training covers topics designed to minimize risks to or from interconnected parties.	1	2	3	4
PR.AT-4.1	The organization's governing body (e.g., the Board or one of its committees) and senior management receive cybersecurity situational awareness training to include appropriate skills and knowledge to: (1) Evaluate and manage cyber risks; (2) Promote a culture that recognizes that staff at all levels have important responsibilities in ensuring the organization's cyber resilience; and (3) Lead by example.	1	2	3	4
PR.AT-4.2	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 to discuss cybersecurity related matters.	1	2	3	4
PR.AT-5.1	The individuals who fulfill the organization's physical and cybersecurity objectives (employees or outsourced) have been informed of their roles and responsibilities.	1	2	3	4
PR.DS-1.1	Data-at-rest is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy.	1	2	3	4
PR.DS-1.2	Controls for data-at-rest include, but are not be restricted to, appropriate encryption, authentication and access control.	1	2	3	4
PR.DS-2.1	Data-in-transit is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy.	1	2	3	4
PR.DS-2.2	Controls for data-in-transit include, but are not be restricted to, appropriate encryption, authentication and access control.	1	2	3	4
PR.DS-3.1	The organization has an asset management process in place and assets are formally managed (e.g., in a configuration management database) throughout removal, transfers, end-of-life, and secure disposal or re-use of equipment processes.	1	2	3	
PR.DS-4.1	The organization maintains appropriate system and network availability, consistent with business requirements and risk assessment.	1	2	3	4
PR.DS-5.1	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-6.1	The organization uses integrity checking mechanisms to verify software, firmware and information integrity, as practicable.	1	2		
PR.DS-7.1	The organization's development, testing and acceptance environment(s) are separate from the production environment, and test data is protected and not used in the production environment.	1	2	3	
PR.DS-8.1	The organization uses integrity checking mechanisms to verify hardware integrity, as practicable.	1			
PR.IP-1.1	The organization establishes and maintains baseline system security configuration standards to facilitate consistent application of security settings to designated information assets.	1	2	3	
PR.IP-1.2	The organization establishes policies, procedures and tools, such as policy enforcement, device fingerprinting, patch status, operating system version, level of security controls, etc., to manage personnel's mobile devices before allowing access to the organization's network and resources.	1	2		
PR.IP-1.3	The organization performs regular enforcement checks to ensure that non-compliance with baseline system security standards is promptly rectified.	1			
PR.IP-2.1	The organization implements a process for Secure System Development Lifecycle for in-house software design and development.	1	2	3	
PR.IP-2.2	The organization implements a process for evaluating (e.g., assessing or testing) externally developed applications.	1	2	3	
PR.IP-2.3	The organization assesses the cyber risks of software prior to deployment.	1	2	3	
PR.IP-3.1	The organization's change management process explicitly considers cyber risks, in terms of residual cyber risks identified both prior to and during a change, and of any new cyber risk created post-change.	1	2	3	
PR.IP-4.1	The organization designs and tests its systems and processes to enable recovery of accurate data (e.g., material financial transactions) sufficient to support normal operations and obligations following a cybersecurity incident.	1	2	3	4

PR.IP-4.2	The organization conducts and maintains backups of information and periodically conduct tests of backups to business assets (including full system recovery) to achieve cyber resilience.	1	2	3	4
PR.IP-4.3	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		
PR.IP-4.4	Recovery point objectives to support data integrity efforts are consistent with the organization's resumption time objective for critical operations.	1	2		
PR.IP-5.1	Physical and environmental security policies are implemented and managed.	1	2	3	4
PR.IP-6.1	Data is maintained, stored, retained and destroyed according to the organization's data retention policy.	1	2	3	4
PR.IP-7.1	A formal process is in place to improve protection processes by integrating lessons learned and responding to changes in the organization's environment.	1	2	3	
PR.IP-8.1	The organization shares appropriate types of information about the effectiveness of its protective measures with appropriate parties.	1	2	3	4
PR.IP-9.1	The organization's business continuity, disaster recovery, crisis management and response plans are in place and managed.	1	2	3	4
PR.IP-9.2	The organization defines objectives for resumption of critical operations.	1	2	3	4
PR.IP-10.1	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 clients.	1	2	3	
PR.IP-10.2	The organization's testing program validates the effectiveness of its cyber resilience framework on a regular basis.	1	2		
PR.IP-10.3	The organization's governing body (e.g., the Board or one of its committees) is involved in testing as part of a crisis management team and is informed of test results.	1			
PR.IP-10.4	The organization promotes, designs, organizes and manages testing exercises designed to test its response, resumption and recovery plans and processes.	1	2	3	4
PR.IP-11.1	The organization conducts background/screening checks on all new employees, as permitted by law.	1	2	3	4
PR.IP-11.2	The organization conducts background/screening checks on all staff at regular intervals throughout their employment, commensurate with staff's access to critical systems or a change in role, as permitted by law.	1	2	3	
PR.IP-11.3	The organization establishes processes and controls to mitigate cyber risks related to employment termination, as permitted by law.	1	2	3	4
PR.IP-12.1	The organization establishes and maintains capabilities for ongoing vulnerability management, including systematic scans or reviews reasonably designed to identify publicly known cyber vulnerabilities in the organization based on the risk assessment.	1	2	3	4
PR.IP-12.2	The organization establishes a process to prioritize and remedy issues identified through vulnerability scanning.	1	2	3	4
PR.IP-12.3	The organization has a formal exception management process for vulnerabilities that cannot be mitigated due to business-related exceptions.	1	2		
PR.IP-12.4	The organization ensures that a process exists and is implemented to identify patches to technology assets, evaluate patch criticality and risk, and test and apply the patch within an appropriate time frame.	1	2	3	4
PR.MA-1.1	Policies, standards and procedures for the maintenance of assets include, but are not limited to, physical entry controls, equipment maintenance and removal of assets.	1	2	3	
PR.MA-2.1	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	1	2	3	
PR.PT-1.1	The organization's audit trails are designed to detect cybersecurity events that may materially harm normal operations of the organization.	1	2	3	4
PR.PT-1.2	The organization's activity logs and other security event logs are reviewed and are retained in a secure manner for an appropriate amount of time.	1	2	3	
PR.PT-2.1	The organization's removable media and mobile devices are protected and use is restricted according to policy.	1	2	3	4

PR.PT-3.1	The organization's systems are configured to provide only essential capabilities to implement the principle of least functionality.	1	2	3	4
PR.PT-4.1	The organization's communications and control networks are protected through applying defense-in-depth principles (e.g., network segmentation, firewalls, physical access controls to network equipment, etc.).	1	2	3	4
PR.PT-5.1	The organization implements mechanisms (e.g., failsafe, load balancing, hot swap) to achieve resilience requirements in normal and adverse situations.	1			
	DETECT				
DE.AE-1.1	The organization identifies, establishes, documents and manages a baseline mapping of network resources, expected connections and data flows.	1	2		
DE.AE-2.1	The organization performs timely collection of relevant data, as well as advanced and automated analysis (including use of security tools such as antivirus, IDS/IPS) on the detected events to: (1) Assess and understand the nature, scope and method of the attack; (2) Predict and block a similar future attack; and (3) Report timely risk metrics.	1	2	3	
DE.AE-3.1	The organization has a capability to collect, analyze, and correlate events data across the organization in order to predict, analyze, and respond to changes in the operating environment.	1	2	3	
DE.AE-3.2	The organization deploys tools, as appropriate, to perform real-time central 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.	1	2	3	
DE.AE-4.1	The organization has a documented process in place to analyze the impact of a material cybersecurity incident (including the financial impact) on the organization as well as across the financial sector, as appropriate, per organization's size, scope, and complexity and its role in the financial sector.	1	2		
DE.AE-5.1	The organization establishes and documents cyber event alert parameters and thresholds as well as rule-based triggers for an automated response within established parameters when known attack patterns, signatures or behaviors are detected.	1	2	3	
DE.CM-1.1	The organization establishes relevant system logging policies that include the types of logs to be maintained and their retention periods.	1	2	3	4
DE.CM-1.2	The organization implements systematic and real-time logging, monitoring, detecting, and alerting measures across multiple layers of the organization's infrastructure (covering physical perimeters, network, operating systems, applications and data).	1	2	3	
DE.CM-1.3	The organization deploys an intrusion detection and intrusion prevention capabilities to detect and prevent a potential network intrusion in its early stages for timely containment and recovery.	1	2	3	4
DE.CM-1.4	The organization implements mechanisms, such as alerting and filtering sudden high volume and suspicious incoming traffic, to prevent (Distributed) Denial of Services (DoS/DDoS) attacks.	1	2	3	
DE.CM-2.1	The organization's controls include monitoring and detection of anomalous activities and potential cybersecurity events across the organization's physical environment and infrastructure, including unauthorized physical access to high-risk or confidential systems.	1	2	3	4
DE.CM-3.1	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	
DE.CM-3.2	The organization performs logging and reviewing of the systems activities of privileged users, and monitoring for anomalies is implemented.	1	2	3	
DE.CM-3.3	The organization conducts periodic cyber attack simulations to detect control gaps in employee behavior, policies, procedures and resources.	1	2		
DE.CM-4.1	The organization implements and manages appropriate tools to detect and block malware from infecting networks and systems.	1	2	3	4
DE.CM-4.2	The organization implements email protection mechanisms to automatically scan, detect, and protect from any attached malware or malicious links present in the email.	1	2	3	4

DE.CM-5.1	The organization implements safeguards against mobile malware and attacks for mobile devices connecting to corporate network and accessing corporate data (e.g., anti-virus, timely patch deployment, etc.).	1	2	3	4
DE.CM-6.1	The organization authorizes and monitors all third-party connections.	1	2	3	4
DE.CM-6.2	The organization collaborates with third-party service providers to maintain and improve the security of external connections.	1	2	3	4
DE.CM-6.3	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-7.1	The organization implements appropriate controls to prevent use of unsupported and unauthorized software.	1	2	3	4
DE.CM-7.2	The organization has policies, procedures and adequate tools in place to monitor, detect, and block access from/to devices, connections, and data transfers.	1	2		
DE.CM-7.3	The organization sets up automatic and real-time alerts when an unauthorized software, hardware or configuration change occurs.	1	2		
DE.CM-7.4	The organization implements web-filtering tools and technology to block access to inappropriate or malicious websites.	1	2	3	4
DE.CM-8.1	The organization conducts periodic vulnerability scanning, including automated scanning across all environments to identify potential system vulnerabilities, including publicly known vulnerabilities, upgrade opportunities, and new defense layers.	1	2	3	4
DE.CM-8.2	The organization conducts, either by itself or by an independent third party, periodic penetration testing and red team testing on the organization's network, internet-facing applications or systems, and critical applications to identify gaps in cybersecurity defenses.	1	2	3	4
DE.DP-1.1	The organization has established and assigned roles and responsibilities for systematic monitoring and reporting processes.	1	2	3	
DE.DP-2.1	The organization's monitoring and detection processes comply with all applicable requirements.	1	2	3	4
DE.DP-3.1	The organization establishes a comprehensive testing program to conduct periodic and proactive testing and validation of the effectiveness of the organization's incident detection processes and controls.	1	2		
DE.DP-4.1	The organization has established processes and protocols to communicate, alert and periodically report detected potential cyber attacks and incident information including its corresponding analysis and cyber threat intelligence to internal and external stakeholders.	1	2	3	4
DE.DP-4.2	The organization tests and validates the effectiveness of the incident reporting and communication processes and protocols with internal and external stakeholders.	1	2		
DE.DP-5.1	The organization establishes a systematic and comprehensive program to periodically evaluate and improve the monitoring and detection processes and controls, as well as incorporate the lessons learned, as the threat landscape evolves.	1	2		
	RESPOND				
RS.RP-1.1	The organization's response plans are in place and executed during or after an incident.	1	2	3	4
RS.CO-1.1	The organization's incident response plan contains clearly defined roles, responsibilities and levels of decision-making authority.	1	2	3	4
RS.CO-1.2	The organization ensures cyber threat intelligence is made available to appropriate staff with responsibility for the mitigation of cyber risks at the strategic, tactical and operational levels within the organization.	1	2		
RS.CO-1.3	The organization's personnel know their roles and responsibilities and order of operations when a response is needed.	1	2	3	4
RS.CO-2.1	The organization's incident response plan describes how to appropriately document and report cyber events and related incident response activities.	1	2	3	4
RS.CO-2.2	In the event of a cybersecurity incident, the organization notifies appropriate stakeholders including, as required, government bodies, self-regulatory agencies or any other supervisory bodies.	1	2	3	4
RS.CO-2.3	The organization's incident response program includes effective escalation protocols linked to organizational decision levels and communication strategies, including which types of information	1	2	3	

	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.				
RS.CO-2.4	The organization's reporting requirements and capabilities are consistent with information-sharing arrangements within the organization's communities and the financial sector.	1	2		
RS.CO-3.1	Information is shared consistent with response plans.	1	2	3	4
RS.CO-3.2	In the event of a cybersecurity incident, the organization shares information in an appropriate manner that could facilitate the detection, response, resumption and recovery of its own systems and those of other financial sector participants through trusted channels.	1	2		
RS.CO-4.1	The organization has a plan to coordinate and communicate with internal and external stakeholders during or following a cyber attack as appropriate.	1	2	3	
RS.CO-5.1	The organization actively participates in multilateral information-sharing arrangements to facilitate a sector-wide response to large-scale incidents.	1	2		
RS.CO-5.2	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.	1	2		
RS.CO-5.3	The organization maintains ongoing situational awareness of its operational status and cybersecurity posture to pre-empt cyber events and respond rapidly to them.	1	2	3	
RS.AN-1.1	Tools and processes are in place to ensure timely detection, alert, and activation of the incident response program.	1	2	3	4
RS.AN-2.1	The organization uses cyber-attack scenarios to determine potential impact to critical business processes.	1	2		
RS.AN-2.2	The organization performs a thorough investigation to determine the nature of a cyber event, its extent, and the damage inflicted.	1	2	3	4
RS.AN-3.1	The organization has the capability to assist in or conduct forensic investigations of cybersecurity incidents and engineer protective and detective controls to facilitate the investigative process.	1	2	3	
RS.AN-4.1	The organization categorizes and prioritizes cybersecurity incident response consistent with response plans and criticality of systems to the enterprise.	1	2	3	
RS.AN-5.1	The organization has established enterprise processes for receiving and appropriately channeling vulnerability disclosures from: (1) Public sources (e.g., 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).	1	2	3	4
RS.AN-5.2	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		
RS.AN-5.3	The organization has established processes to implement vulnerability mitigation plans, as well as validate their completion and effectiveness.	1	2	3	4
RS.MI-1.1	The organization contains cybersecurity incidents in a timely manner.	1	2	3	4
RS.MI-1.2	The organization's procedures include containment strategies and notifying potentially impacted third parties, as appropriate.	1	2	3	4
RS.MI-2.1	The organization mitigates cybersecurity incidents in a timely manner.	1	2	3	4
RS.MI-3.1	The organization's incident response plan identifies requirements for the remediation of any identified weaknesses in systems and associated controls.	1	2	3	4
RS.MI-3.2	Vulnerabilities identified as a result of a cybersecurity incident are mitigated or documented by the organization as accepted risks and monitored.	1	2	3	
RS.IM-1.1	The organization's incident response plans are actively updated based on current cyber threat intelligence, information-sharing and lessons learned following a cyber event.	1	2	3	4

RS.IM-1.2	The results of the testing program are used by the organization to support ongoing improvement of its cyber resilience.	1	2		
RS.IM-1.3	The organization's cyber resilience and incident response programs have processes in place to incorporate lessons learned from cyber events that have occurred within and outside the organization.	1	2	3	
RS.IM-2.1	The organization periodically reviews response strategy and exercises and updates them as necessary, based on: (1) Lessons learned from cybersecurity incidents that have occurred (both within and outside 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; and (5) New technological developments.	1	2	3	4
	RECOVER				
RC.RP-1.1	The organization executes its recovery plans, including incident recovery, disaster recovery and business continuity plans, during or after an incident to resume operations.	1	2	3	4
RC.RP-1.2	Organization's recovery plans are executed by first resuming critical services and core business functions, and without causing any potential concurrent and widespread interruptions to interconnected entities and critical infrastructure, such as energy and telecommunications.	1	2	3	4
RC.RP-1.3	The recovery plan includes a minimum recovery time for the sector critical systems.	1	2		
RC.RP-1.4	The recovery plan includes recovery of clearing and settlement activities after a wide-scale disruption with the overall goal of completing material pending transactions on the scheduled settlement date.	1	2		
RC.RP-1.5	The recovery plan includes recovery of resilience following a long term loss of capability (e.g., site or third party) detailing when the plan should be activated and implementation steps.	1	2		
RC.RP-1.6	The recovery plan includes plans to come back for both traditional and highly available (e.g., cloud) infrastructure.	1	2		
RC.IM-1.1	The organization refines its cyber resilience and incident response plans by actively identifying and incorporating crucial lessons learned from: (1) cybersecurity incidents that have occurred within the organization; (2) Cybersecurity assessments and testing performed internally; and (3) Widely reported events, industry reports and cybersecurity incidents that have occurred outside the organization.	1	2	3	
RC.IM-2.1	The organization periodically reviews recovery strategy and exercises and updates them as necessary, based on: (1) Lessons learned from cybersecurity incidents that have occurred (both within and outside 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; and (5) New technological developments.	1	2		
RC.CO-1.1	The organization's governing body (e.g., the Board or one of its committees) ensures that a communication plan exists to notify internal and external stakeholders about an incident, as appropriate.	1	2	3	4
RC.CO-1.2	The organization promptly communicates the status of recovery activities to regulatory authorities and relevant external stakeholders, as appropriate.	1	2	3	4
RC.CO-2.1	Actionable and effective mitigation techniques are taken and communicated appropriately to restore and improve the organization's reputation after an incident.	1	2	3	4
RC.CO-3.1	The organization timely involves and communicates the recovery activities, procedures, cyber risk management issues to the appropriate governing body (e.g., the Board or one of its committees), senior management and relevant internal stakeholders.	1	2	3	4
	SUPPLY CHAIN / DEPENDENCY MANAGEMENT				

DM.ID-1.1	The organization has integrated its internal dependency management strategy into the overall strategic risk management plan.	1			
DM.ID-1.2	The organization monitors the effectiveness of its internal dependency management strategy.	1			
DM.ID-1.3	The organization ensures appropriate oversight of and compliance with the internal dependency management strategy implementation.	1			
DM.ID-1.4	The organization has established and applies appropriate controls to address the inherent risk of internal dependencies.	1			
DM.ID-2.1	Roles and responsibilities for internal dependency management are defined and assigned.	1			
DM.ED-1.1	The organization has integrated its external dependency management strategy into the overall cyber risk management plan.	1	2		
DM.ED-1.2	The organization monitors the effectiveness of its external dependency management strategy to reduce cyber risks associated with external dependencies.	1	2		
DM.ED-1.3	The organization ensures appropriate oversight and compliance with the external dependency strategy implementation.	1	2		
DM.ED-2.1	The organization has established policies, plans, and procedures to identify and manage cyber risks associated with external dependencies throughout those dependencies' lifecycles in a timely manner, including sector-critical systems and operations.	1	2	3	4
DM.ED-2.2	The organization's dependency management policies, plans, and procedures are regularly updated.	1	2	3	4
DM.ED-2.3	The organization's dependency management policies, plans, and procedures have been reviewed and approved by appropriate organizational stakeholders.	1	2	3	4
DM.ED-2.4	Dependency management processes may allow the organization to the adopt security program(s) of its "affiliate(s)" as long as such program provides an appropriate level of control and assurance.	1	2		
DM.ED-2.5	The organization's dependency management process identifies third-party relationships that are in place, including those relationships that were established without formal approval.	1	2	3	
DM.ED-3.1	Roles and responsibilities for external dependency management are defined and assigned.	1	2	3	4
DM.ED-3.2	Responsibilities for ongoing independent oversight (external) of third-party access are defined and assigned.	1	2	3	
DM.ED-4.1	The organization ensures that cyber risks associated with external dependencies are consistent with cyber risk appetite approved by an appropriate governing body (e.g., the Board or one of its committees).	1	2	3	4
DM.ED-4.2	The organization has established and applies appropriate policies and controls to address the inherent risk of external dependencies to the enterprise and the sector, if appropriate.	1	2	3	4
DM.ED-4.3	The organization conducts a risk assessment to define appropriate controls to address the cyber risk presented by each external partner, implements these controls, and monitors their status throughout the lifecycle of partner relationships.	1	2		
DM.ED-4.4	The organization has a documented third-party termination/exit strategy to include procedures for timely removal of the third-party access when no longer required.	1	2		
DM.ED-4.5	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		
DM.ED-5.1	The organization has identified and monitors the organizational ecosystem of external dependencies for assets/systems that are critical to the enterprise and the financial services sector.	1			
DM.ED-5.2	The organization maintains a current, accurate, and complete listing of all external dependencies and business functions, including mappings to supported assets and business functions.	1	2		
DM.ED-5.3	The organization has prioritized functions, activities, products, and services provided by external dependencies based on criticality.	1	2		
DM.ED-5.4	The organization has prioritized external dependencies according to their criticality to the supported business functions, enterprise mission, and to the financial services sector.	1	2		
DM.ED-6.1	The organization has documented minimum cybersecurity requirements for critical third parties that, at a minimum, meet cybersecurity practices of the organization.	1	2	3	4

DM.ED-6.2	The organization's contracts require third parties to implement minimum cybersecurity requirements and to maintain those practices for the life of the relationship.	1	2	3	4
DM.ED-6.3	Minimum cybersecurity requirements for third parties include how the organization will monitor security of its external dependencies to ensure that requirements are continually satisfied.	1	2	3	4
DM.ED-6.4	Minimum cybersecurity requirements for third parties include consideration of whether the third party is responsible for the security of the organization's confidential data and of geographic limits on where data can be stored and transmitted.	1	2	3	4
DM.ED-6.5	Minimum cybersecurity requirements for third parties include how the organization and its suppliers and partners will communicate and coordinate in times of emergency, including: 1) Joint maintenance of contingency plans; 2) Responsibilities for responding to cybersecurity incident; 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 potential impact of a cyber event into their BCP process and ensure appropriate resilience capabilities are in place.	1	2	3	4
DM.ED-6.6	Minimum cybersecurity requirements for third parties identify conditions of and the recourse available to the organization should the third party fail to meet their cybersecurity requirements.	1	2	3	4
DM.ED-6.7	Minimum cybersecurity requirements for third parties cover the entire relationship lifecycle, including return or destruction of data during cloud or virtualization use and upon relationship termination.	1	2	3	4
DM.ED-7.1	The organization has a formal program for third-party due diligence and monitoring.	1	2	3	4
DM.ED-7.2	The organization conducts regular third-party reviews for critical vendors to validate that appropriate security controls have been implemented.	1	2	3	
DM.ED-7.3	A process is in place to confirm that the organization's third-party service providers conduct due diligence of their own third-parties (e.g., subcontractors).	1	2		
DM.ED-7.4	A process is in place to confirm that the organization's third-party service providers conduct periodic resiliency testing or justify why it is not needed.	1			
DM.RS-1.1	The organization has an enterprise-wide cyber resilience (including business continuity, and incident response) strategy and program.	1	2	3	4
DM.RS-1.2	The cyber resilience strategy and program are based on the organization's enterprise-wide cyber risk management strategy that addresses the risks that the organization may present to other critical infrastructure sectors and the risk that the organization may present to other firms in the financial sector.	1	2		
DM.RS-1.3	The cyber resilience program ensures that the organization can continue operating critical business functions and deliver services to stakeholders during cybersecurity incidents and cyber attacks (e.g., propagation of malware or corrupted data).	1	2		
DM.RS-2.1	The organization has incorporated its external dependencies and critical business partners into its cyber resilience (e.g., incident response, business continuity, and disaster recovery) strategy, plans, and exercises.	1	2		
DM.RS-2.2	The organization's cyber resilience strategy addresses the organization's obligations for performing core business functions including those performed for the financial sector as a whole, in the event of a disruption, including the potential for multiple concurrent or widespread interruptions and cyber attacks on multiple elements of interconnected critical infrastructure, such as energy and telecommunications.	1	2		
DM.RS-2.3	The organization designs and tests its cyber resilience plans, and exercises to support financial sector's sector-wide resilience and address external dependencies, such as connectivity to markets, payment systems, clearing entities, messaging services, etc.	1	2		
DM.RS-2.4	The organization periodically identifies and tests alternative solutions in case an external partner fails to perform as expected.	1	2		
DM.RS-2.5	When planning and executing incident response and recovery activities, the organization takes into consideration sector-wide impact of its systems and puts a priority on response and recovery activities for those systems ahead of the other systems.	1	2		
DM.BE-1.1	The cyber risk strategy identifies and communicates the organization's role as it relates to other critical infrastructures and as a component of the financial services sector.	1	2		

DM.BE-1.2	A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across other sectors the institution depends upon.	1	2
DM.BE-2.1	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	2
DM.BE-2.2	The organization has prioritized monitoring of systems according to their criticality to the supported business functions, enterprise mission, and to the financial services sector.	1	2
DM.BE-3.1	Cyber resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).	1	