Financial Services - Sector Specific Goals

August 2026

U.S. Department of the Treasury

August 24, 2026

To reduce cybersecurity risks to our nation's critical infrastructure, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) collaborated with various Sector Risk Management Agencies (SRMAs) to develop sector-specific cybersecurity performance goals. U.S. Department of the Treasury (Treasury), as the designated SRMA for the financial services sector, participated in the initial group of SRMAs to deliver sector-specific cybersecurity goals.

Following the release of the cross-sector cybersecurity performance goals (CPGs) and most recent update in December 2025, which set a baseline of cybersecurity practices across critical infrastructure, select critical infrastructure sectors started developing specific goals based on their own unique sectoral requirements. The Financial Services-Sector Specific Goals (FS-SSGs) for cybersecurity are intended to address gaps between the existing CISA CPGs and financial services sector's best known cybersecurity risk management practices. Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) worked closely with the Financial Services Sector Coordinating Council (FSSCC) to develop these goals, which aim to enhance the sector's cybersecurity posture. FSSCC led the development of these sector-specific goals with Treasury and CISA's coordination and input.

These voluntary FS-SSGs are also intended to help institutions align their cybersecurity practices with the National Institute of Standards and Technology Cybersecurity Framework 2.0. The financial sector's resiliency remains highly dependent on other critical industries, sectors, and third parties' security practices. FS-SSGs are particularly beneficial in assisting small to medium sized financial institutions and third-party entities in prioritizing cybersecurity practices for their own firms and establishing baseline cybersecurity goals.

This document is provided as a voluntary guide for informational purposes only. Use of this document is neither required by nor guarantees compliance with federal, state, or local laws. This document is not intended to and does not create any new regulatory obligation or expectation. The information presented may not be applicable or appropriate for all financial institutions and organizations. This document is not an exhaustive or definitive source of all the practices needed to protect against cybersecurity risks. Mentions of trade names or specific commercial profiles or products do not constitute endorsement or recommendation for use.

Overview of Financial Services – Sector Specific Goals

Executive Summary

The financial services sector is one of the most technologically advanced and globally competitive sectors of the U.S. economy, supported by decades of investment, innovation, and strong cybersecurity risk management. However, the sector's deep interconnectedness with other critical third-party service providers—many of which do not operate at the same maturity level—introduces third-party risks that can impact not only financial institutions but the sector as a whole.

To address these risks without adding new requirements or expanding regulation, the U.S. Treasury and the FSSCC[1] have developed voluntary FS-SSGs to complement the CISA CPGs 2.0. These goals create a risk-based pathway to help financial institutions' third parties calibrate their cybersecurity practices to a subset of existing Gramm-Leach-Bliley-Act aligned (GLBA) expectations already reflected in Tier 4 of the Cyber Risk Institute (CRI) Profile. The FS-SSGs were provided to members of the Financial and Banking Information Infrastructure Committee[2] for their awareness.

The FS-SSGs **do not** introduce new obligations, requirements, or supervisory expectations. Instead, they draw exclusively from a subset of the Tier 4 diagnostic statements in the CRI Profile and provide a clear, scalable on ramp from CISA's CPGs 2.0 toward practices already expected of regulated financial institutions under GLBA. This approach strengthens sector-wide resilience by improving clarity—not by increasing regulation.

PURPOSE OF THE FS-SSGS

The FS-SSGs are designed to:

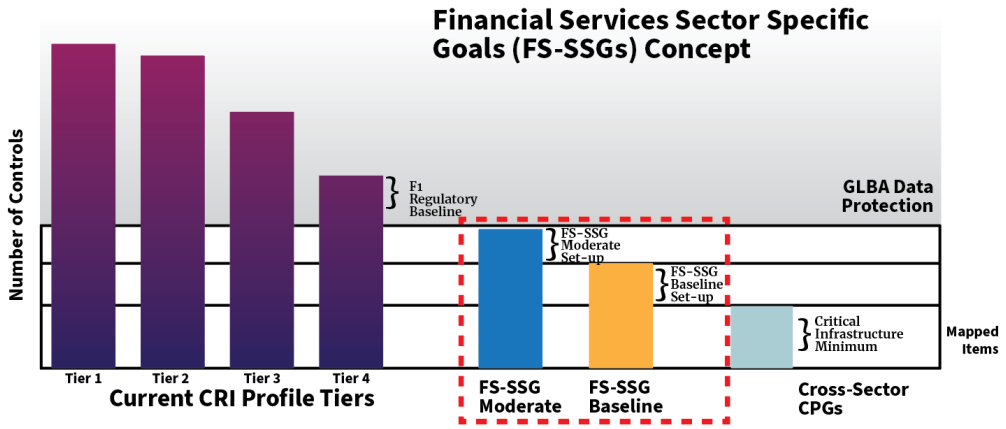
- Strengthen supply-chain security, a known national vulnerability;
- Reduce the risk of cascading failures across critical infrastructure;
- Support a more efficient and predictable ecosystem for financial institutions and vendors;
- Provide clarity for smaller firms and fintech innovators, reducing compliance confusion; and
- Leverage industry leadership to avoid heavier regulatory alternatives.

The following graphic illustrates how the FS-SSGs provide a clear, efficient stepping stone from the CISA CPGs[3] —intended for all critical infrastructure—to the minimum GLBA requirements already reflected in Tier 4 of the CRI Profile.[4] This approach strengthens third-party resilience without adding regulatory burden on financial institutions, and

1 https://fsscc.org/
2 https://www.fbiic.gov/
3 https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
4 https://cyberriskinstitute.org/cri-profile-overview/
5 https://www.nist.gov/cyberframework

requirements already reflected in Tier 4 of the CRI Profile.[4] This approach strengthens third-party resilience without adding regulatory burden on financial institutions, and leverages a voluntary, industry-developed and -led standard aligned to the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0.[5]

Figure: Diagram of Financial Services-Sector Specific Goals



By raising maturity across third parties in a voluntary, risk-aligned, and scalable way, Treasury and FSSCC can improve third-party maturity across the U.S. financial system—supporting economic growth, protecting American businesses and consumers, and enhancing national resilience without expanding regulation.

METHODOLOGY

To develop the FS-SSGs, the FSSCC analyzed seven sources ranging from industry standards and frameworks to financial institutions' individual best practices for managing third-party cybersecurity. This analysis identified common minimum expectations appropriate for organizations supporting financial institutions that sit below minimum requirements for regulated entities:

- **FS-SSG "Baseline":** Appropriate for financial institutions to expect of service providers managing non-sensitive data or performing non-critical functions.
- **FS-SSG "Moderate":** Appropriate for financial institutions to expect of service providers handling sensitive data or supporting critical business operations.

The FS-SSG "Baseline" and "Moderate" levels enable organizations to adopt controls proportionate to the services they or their third parties provide (see table below).

4 https://cyberriskinstitute.org/cri-profile-overview/
5 https://www.nist.gov/cyberframework

Number of Controls for Financial Services - Sector Specific Goals								
	Govern[a]	Identify	Protect	Detect	Respond	Recover	Extend[b]	Totals
CISA CPGs	10	15	32	8	4	3	9	**81**
FS-SSG "Baseline"	16	17	46	11	10	4	9	**113**
FS-SSG "Moderate"	27	32	59	16	11	4	18	**167**
Financial Institution Baseline Expectation	64	37	49	14	12	10	12	**208**

a Govern is a function in the NIST CSF version 2.0 and the CRI Profile version 2.0.

b Extend is a function included in the CRI Profile and the content maps to the NIST CSF version 2.0's "Govern" function.

The primary distinctions between these two levels include the sensitivity of the data that a financial institution provides to a third-party service provider and the criticality of the services performed. The FS-SSG Baseline level is relevant for third parties that are providing basic services that do not include sensitive data (e.g., personally identifiable information) or critical business functions. The FS-SSG Moderate level is relevant for third parties that are providing services that involve sensitive data and/or critical business functions.

Financial institutions generally have different cybersecurity requirements for third parties depending on the type of data or service that is involved. For example, a financial institution might have minimum requirements if the entity is handling non-sensitive data, but more stringent requirements if the entity is handling critical data or providing a function for critical services.

The intent of the FS-SSGs is to increase the level of maturity of the financial services sector, while recognizing that even the smallest financial institutions have a high level of regulatory expectations as demonstrated in the diagnostic statements in Tier 4 of the CRI Profile. The FS-SSGs use many of the same Tier 4 control objectives, or diagnostic statements, to identify the FS-SSG "Baseline" and FS-SSG "Moderate" levels. The FS-SSGs identify baseline goals for supply chain risk management, which is considered a key risk to the sector.

Financial Services
Sector Specific Goals (FS-SSG) ver. 2.0

FS SSG Id	FS SSG Control Objective	CPG / FS-SSG "Stepping Stones"			Implementation Guidance	Examples of Effective Evidence	NIST CSF v2 Reference	CRI Profile Id
		CISA CS-CPGs v2	FS-SSG "Baseline"	FS-SSG "Moderate"				
	GOVERN							
FS SSG.001	**Governance alignment:** Technology and cybersecurity strategies, architectures, and programs are formally governed to align with and support the organization's mission, objectives, priorities, tactical initiatives, and risk profile.	**1.B**	**Yes**	**Yes**	Describe how the organization's mission, objectives, and activities establish priorities for the technology and cybersecurity strategies, architectures, and programs and communicates those priorities. Response should include documentation, such as the organizational mission statement, cybersecurity and technology program, strategies, architectures, aligned target operating model (i.e., desired state of operations considering the organization's role in critical infrastructure) and related documents supporting the establishment and communication of priorities for the organizational mission, objectives, and activities.	- Organizational mission statement - Cybersecurity program, strategy and framework - Technology program, strategy and framework - Related description of services (e.g., service catalog, including both business and IT services) provided by involved teams - Target operating model (i.e., desired state of operations considering the organization's role in critical infrastructure) - Mission statement - Organizational charts - Roles and responsibilities	GV.OC-01	GV.OC-01.01
FS SSG.002	**Legal, contractual, and regulatory obligations:** The organization's technology and cybersecurity strategy, framework, and policies align and are consistent with the organization's legal, statutory, contractual, and regulatory obligations and ensure that compliance responsibilities are unambiguously assigned.	**1.B**	**Yes**	**Yes**	The Gramm-Leach-Bliley Act and its implementing regulations, including the Guidelines Establishing Standards for Safeguarding Customer Information is the seminal set of legal expectations as it relates to information security for financial institutions in the United States. Other jurisdictions will have additional legal and regulatory obligations in place. Regulatory guidance and/or legal requirements may apply based on products, services, and legal structure. Furthermore, organizations will have contractual obligations with vendors, government agencies, and other third-party service providers that should be tracked for compliance with established responsibilities. Provide information on how new or enhanced technology and cybersecurity regulations and contractual obligations are published (trigger event), and how technology and cybersecurity strategies, frameworks, and policies are reviewed and updated to ensure regulatory and contractual obligation alignment. Responses should describe any existing efforts within the organization that may map regulatory and contractual requirements to existing policies, procedures, and controls. Provide information regarding any the organizations processes for identifying, tracking, and overseeing regulatory and contractual requirements. Roles and responsibilities should be clearly defined and unambiguously assigned for technology and cybersecurity. Provide information on how the organization ensures responsibilities are unambiguously assigned (e.g., compliance responsibility assignment matrix, RACI charts).	- Cybersecurity policy and standards (including approval and revision history) - Policy roadmap or process document - Evidence of legal and regulatory updates (e.g., working group action tracker) - Laws and regulations assessment process, including how laws and regulations are documented in existing policies - Board reports - Relevant Board or committee meeting agendas and minutes - Annual goals plans - Responsibility assignment matrix/RACI charts that identify compliance responsibilities - Organization charts with compliance organization units identified	GV.OC-03	GV.OC-03.01
FS SSG.003	**Data Privacy Policy:** The organization implements and maintains a documented policy or policies that address customer data privacy that is approved by a designated officer or the organization's appropriate governing body (e.g., the Board or one of its committees).	--	**Yes**	**Yes**	Describe how the various policies and standards in place are designed to protect customer privacy and comply with local laws. Indicate how these documents describe security and safeguarding of information generated and obtained in the course of executing business activities. Identify who in the organization is responsible for maintaining privacy-related programs, documents, and compliance activities.	- Relevant Board or committee (e.g., Risk Committee) meeting agendas and minutes - Information Security Program supporting Information - Data privacy policies - Periodic review and approval process for policies and procedures - Data classification matrix - Organizational chart of privacy office, showing Chief Privacy Officer and reporting lines	GV.OC-03	GV.OC-03.02

FS SSG.004	**Critical service dependencies:** The organization identifies, assesses, and documents the key dependencies, interdependencies, and potential points of failure to support the delivery of critical services (e.g., systems, business processes, workforce, third parties, facilities, etc.)	--	--	**Yes**	In order to plan and assess for enterprise resilience, the organizations should identify, assess, and document internal and external dependencies to understand upstream and downstream affects of potential points of failure to critical services (systems, business processes, third parties, facilities, etc.). Responses should describe the organizations processes to identify, assess, and document internal and external dependencies. Dependency evaluation and management processes should consider internal and external dependencies for critical services (information systems, data processing facilities, third party providers, business processes, etc.). Include considerations of backup systems and facilities, and third party service providers on retainer contracts.	- Inventory of critical internal and external dependencies, business functions, systems, and third parties - Identification criteria of critical external dependencies and related business functions - Resiliency management policy, standard, and procedures - Third-party security policy, standard, and procedures - Third-party risk management program - Critical third-party reporting or other related reporting - Critical operations inventory	GV.OC-05	GV.OC-05.01
FS SSG.005	**Alignment of resilience measures:** The organization defines objectives (e.g., Recovery Time Objective, Maximum Tolerable Downtime, Impact Tolerance) for the resumption of critical operations in alignment with business imperatives, stakeholder obligations, and critical infrastructure dependencies.	--	--	**Yes**	Describe how the organization defines objectives for resumption of critical operations (recovery time objectives, recovery point objectives). Organizations should establish an Impact Tolerance objective for critical business services that defines the maximum tolerable level and duration for a disruption. Describe how the Recovery Time Objective, Maximum Tolerable Downtime, and Impact Tolerance are designed to improve the organization's operational resilience. Include information on the organization's business impact analysis, the scope of critical business processes, and prioritization for recovery, among other details. Provide information on the framework and tools utilized to define objectives. Provide information on frequency of assessment and any risk-based criteria.	- Business continuity/resiliency policies, procedures, and plans - Recovery time objectives (RTO) - Recovery point objectives (RPO) - Impact Tolerance analyses - Critical operations inventory - Roles and responsibilities for staff involved in resumption of critical operations - Recent business impact analysis	GV.OC-05	GV.OC-05.03
FS SSG.006	**Risk management strategy approval:** Technology and cybersecurity risk management strategies and frameworks are approved by the governing authority (e.g., the Board or one of its committees) and incorporated into the overall business strategy and enterprise risk management framework.	--	--	**Yes**	The organization's technology and cybersecurity risk management strategies and frameworks should be a key consideration in all business strategies, practices, policies, and procedures. The technology and cybersecurity risk management strategies should align with long-term business strategies and the technologies to support these strategies. Management can support an enterprise information security program and enterprise risk management framework by setting a strong security culture that begins with board involvement and ongoing cybersecurity awareness training that is expected at all levels of management and staff. Include information about the organization's technology and cybersecurity risk management strategies and frameworks. Document the approval of the strategies and frameworks by the Board (or one of its committees) and outline how they incorporate business strategy and links to the enterprise risk management framework. For example, the cybersecurity risk management framework should be part of the organization's overall enterprise risk management framework. Describe how that framework is established and executed for cybersecurity risk management.	- Technology and cybersecurity risk management strategies and frameworks, including evidence of approval by the Board (or one of its committees) or other appropriate governing authority - Enterprise risk management frameworks setting authority framework - Policies, standards, procedures, and guidelines specific to technology and cyber risk management - Organizational chart to demonstrate functional roles, responsibilities, and independence - Relevant Board and committee (e.g., cyber risk strategy committee, technology steering committee, etc.) meeting minutes and approvals where technology and cyber risk management strategy is discussed	GV.RM-01	GV.RM-01.01
FS SSG.007	**Technology and cybersecurity program objectives:** The organization has established, and maintains, technology and cybersecurity programs designed to protect the confidentiality, integrity and availability of its information and operational systems, commensurate with the organization's risk appetite and business needs.	**1.B**	**Yes**	**Yes**	Describe how the technology and cybersecurity programs are maintained, managed, and governed. Provide examples of how the programs assess and manage processes, activities, or systems, to ensure that they are operating effectively and work with all of the organization's business functions to understand and manage the risks. Describe the technology and cybersecurity programs performance measures and risk indicators (e.g., KRIs, KPIs, and KCIs), and how the program addresses inherent risk to the organization. Describe how the programs are reviewed and approved annually at the Board Risk Committee. Describe how the organization strengthens the technology and cybersecurity capabilities in line with the organization's risk appetite and reducing the likelihood of a successful cyber-attack or service disruption. Provide examples of how programs align to industry recognized cyber frameworks and standards (e.g., the CRI Profile, NIST, ISO, FFIEC CAT, etc.)	- Technology and Cybersecurity/Information Security Programs - Program steering committee agenda and minutes - Relevant Board or committee (e.g., Risk Committee) meeting agendas and minutes - Technology and cybersecurity action plans (layered security approach) - Technology and cybersecurity key performance indicators and key risk indicators	GV.RM-01	GV.RM-01.03

FS SSG.008	**Risk management program components:** Technology and cybersecurity risk management programs incorporate risk identification, measurement, monitoring, and reporting.	--	--	**Yes**	The organization's technology and cyber risk management programs should incorporate defined and structured processes to the likelihood and impact of threats and identify mitigating controls. The program should also identify inherent risk and measure, monitor, and report the effectiveness of controls and residual risk. Describe how the technology and cyber risk management programs incorporate risk identification, measurement, monitoring, and reporting. Provide the organization's enterprise risk management framework where there is an available risk and control library, how risk and control assessments are completed (identification of key risks and mitigating controls) and monitoring and reporting of such risks. Include any additional organization-specific tools to measure technology and cyber risk reductions.	- Technology and cyber risk management strategies and frameworks and methodologies - Description of risk assessment and risk management processes - Control libraries - Relevant Board and committee meeting agendas and minutes - Technology and cyber risk reports and briefings - Risk control monitoring and self-assessment material (e.g., process maps, GRC reports, etc.) - Technology and cybersecurity dashboards and/or metrics (monthly, quarterly, annually) - Reports demonstrating threat intelligence capability to identify new and shifting risks/adversaries/vulnerabilities - Organization-specific tools or processes to reduce identified risks	GV.RM-01	GV.RM-01.04
FS SSG.009	**Third-party incident coordination:** The organization establishes minimum requirements for its third-parties that include how the organizations will communicate and coordinate in times of emergency, including: 1) Joint maintenance of contingency plans; 2) Responsibilities for responding to incidents, including forensic investigations; 3) Planning and testing strategies that address severe events in order to identify single points of failure that would cause wide-scale disruption; and 4) Incorporating the potential impact of an incident into their BCM process and ensure resilience capabilities are in place.	**1.E. 5A**	**Yes**	**Yes**	As referenced in EX.CN-02.01, the organization has documented minimum cybersecurity requirements for third parties. Describe how minimum cybersecurity requirements for critical third parties include how the organization and its suppliers and partners will communicate and coordinate in times of emergency. Provide detail for each of the four areas highlighted in the full Diagnostic Statement. The organization's incident response program should address notification and communication with third parties regarding incidents at the third party that might impact the organization. Similarly, contracts with third parties should stipulate incident reporting requirements to ensure there are clearly documented processes and accountability for communicating and coordinating during times of emergencies.	- Third-party security policy, standard, and procedures - Third-party risk management program - Contract guidance - Contract clauses - Contract reporting - Contingency plans - Escalation matrix - Testing strategies - Related third-party reporting - Shared security responsibility model (SSRM)	GV.RM-05	GV.RM-05.02
FS SSG.010	**Risk management processes:** Technology and cybersecurity risk management and risk assessment processes and methodologies are documented and regularly reviewed and updated to address changes in the risk profile and risk appetite, the evolving threat environment, and new technologies, products, services, and interdependencies.	--	--	**Yes**	Technology and cybersecurity-related risks should be identified, reviewed, and analyzed as part of the organization's risk management processes. New products and services, as well as outsourced relationships, have the potential of introducing new or expanding existing technology and cybersecurity risks. Such risks should be evaluated to determine whether appropriate risk management processes are in place. On a regular basis, senior management should review and update risk management standards, practices, and procedures to be reflective of new technologies, products, services, and interdependencies (e.g., AI and quantum risks, cloud, and cloud third parties). In addition, the threat environment is highly dynamic and prominent threats can necessitate revisiting these technology and cybersecurity risk management and risk assessments. Risk assessments should be updated with the most current information regarding widely known risks and risk management practices to assist management and the board in making informed decisions. Provide evidence that the technology and cyber risk assessment processes and methodologies are documented and updated regularly. Demonstrate how risks are routinely addressed through management reporting of current and/or top and emerging risks within the organization to the Board and/or relevant committee (e.g., Board Risk Committee). Provide evidence that a technology and cybersecurity risk update is routinely provided by management to the Board Risk Committee.	- 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-06	GV.RM-06.01

FS SSG.011	**Standard practices use:** 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.	--	--	**Yes**	Provide information on the use of technical security standards, architectures, processes, and practices to ensure the security of applications and infrastructure. Include evidence of technical industry standards used throughout technology and cybersecurity risk management (e.g., SABSA, NIST 800-53, ISO 27001, etc.) Describe and evaluate how these are defined and maintained.	- Security policy and standards documentation - Third-party security standards, processes, and reports - Application, security, and/or infrastructure security standards, processes, and reports - Secure system development standards and processes - Security testing standards, processes, and reports - Other related policies, standards, and procedures (including documentation of security policy reviews) - Evidence of technical industry frameworks standards used throughout system development lifecycle (e.g., SABSA, NIST 800-53, ISO 27001, etc.) - Risk management and risk assessment standards	None	GV.RM-08.03
FS SSG.012	**Designated organization and third-party responsibilities:** The organization clearly defines, and includes in contractual agreements, the division of cybersecurity and technology risk management responsibilities between the organization and its third parties (e.g., a Shared Responsibilities Model).	**1.A, 1.E**	**Yes**	**Yes**	Management must require third-party service providers by contract to implement appropriate measures designed to meet the organization's minimum cybersecurity requirements and the objectives of regulatory guidelines. Provide detail on how the organization establishes and maintains contracts with third-party service providers to define the risk management roles and responsibilities between the organization and service provider, including the division of cybersecurity and technology risk management. Review existing contract and boilerplate language to confirm whether additional contractual language is required or should be expanded upon. Provide information on how the organization establishes a shared responsibilities model or similar mechanism to ensure that all appropriate responsibilities are documented, managed, unambiguously assigned, and shared responsibilities are clear between a customer and third party service provider.	- Third-party security policy, standard, and procedures - Third-party risk management program - Vendor management security policy, standard, and procedures - Vendor management program - Contract guidance - Contract clauses - SSRM documentation	GV.SC-02	GV.SC-02.01
FS SSG.013	**Third-party inventory and risk-ranking:** The organization regularly identifies, inventories, and risk-ranks third-party relationships that are in place, and addresses any identified relationships that were established without formal approval.	--	--	**Yes**	The organization should identify all third-party service providers (e.g., core processing, online and mobile banking, settlement activities, disaster recovery services, cloud service providers, application programming interfaces (API), and other emerging technologies) and categorize them with respect to risk. Describe how the organization's third-party risk management program and process identifies, tracks, and inventories third-party relationships that are in place, including those relationships that were established without formal approval. One means to detect new relationships which bypassed the formal approval process is to reconcile the accounts payable with a listing of managed third-party vendors. Procedures can also be implemented to disallow procurement of certain vendor services without the approval of the security and/or technology functions. Highlight the process and any tools used. Understanding what third-party relationships are in place including those that have been established without formal approval can be useful for identifying potential risks and threats as well as aiding response activities during an information security event.	- Third-party security policy, standard, and procedures - Third-party risk management program - Inventory of third-parties and/or identified critical vendors - Business Impact Analysis - Third-party risk assessment - Related reporting and examples	GV.SC-04	GV.SC-04.01

FS SSG.014	**Resilience program and external dependencies:** The organization's resilience strategy, plans, tests, and exercises incorporate its external dependencies and critical business partners.	--	--	**Yes**	The organization's third-party risk management strategy should be incorporated into the resilience strategy. Describe how the organization has incorporated its third parties and critical business partners into its resilience (e.g., incident response, business continuity, and disaster recovery) strategy, plans, tests, and exercises.	- Security incident response policy, standard, and procedures - Business continuity/resilience policy, standard, and procedures - Incident response examples or playbooks - Third-party testing plan and after-action reports - Third-party security policy, standard, and procedures - Third-party risk management program - Critical third-party identification processes - Critical third-party inventory	GV.SC-08	GV.SC-08.01
FS SSG.015	**Technology and cybersecurity risk management accountability:** The governing authority (e.g., the Board or one of its committees) oversees and holds senior management accountable for implementing the organization's technology and cybersecurity risk management strategies and frameworks.	--	--	**Yes**	The Board (or a board committee) is responsible for the oversight of the organization's technology and cybersecurity risk management program and should ensure compliance with the requirements of the programs by the organization's management, employees, and contractors. The appropriate governing authority may differ by organization (e.g., Senior Management, Executive Management, etc.) but refers to those who should be held accountable for implementing the organization's technology and cybersecurity risk management strategies and frameworks. Accountability requires clear lines of reporting, clear communications, communication of expectations, and the delegation and judicious use of appropriate authority to ensure appropriate compliance with the organization's policies, standards, and procedures. Include information about relevant board and committee charters (e.g., Board Risk Committee Charter), annual approval of the technology and cybersecurity risk management strategies and frameworks (in addition to the information security program), and terms of reference for any other committees as delegated by the board to review/approve. Describe any related regulatory reporting of the technology and cybersecurity risk management strategies and frameworks. Provide organizational charts to identify responsible/accountable executives.	- Technology and cybersecurity risk management strategies and frameworks, including evidence of approval by appropriate governing authority - Policies, standards, controls, procedures, and guidelines specific to technology and cybersecurity risk management - Relevant Board and committee (e.g., Board Risk, IT Steering, and other oversight committees) charters and meeting minutes, including those where senior management with accountability for cybersecurity strategy are required to present on effectiveness/implementation - Gramm-Leach-Bliley Act (GLBA) compliance report - Organizational charts to demonstrate accountable individuals, roles, and responsibilities for technology and cybersecurity risk management - Senior management scorecards on operating effectiveness, including KPIs and KRIs	GV.RR-01	GV.RR-01.01
FS SSG.016	**Cybersecurity Officer designation:** The organization has designated a qualified Cybersecurity Officer (e.g., CISO) who is responsible and accountable for developing a cybersecurity strategy, overseeing and implementing its cybersecurity program, and enforcing its cybersecurity policy.	**1.A**	**Yes**	**Yes**	Accountability requires clear lines of reporting, clear communication of expectations, and the delegation and judicious use of appropriate authority to ensure compliance with the organization's policies, standards, and procedures. Provide information on the designated and qualified Cybersecurity Officer (e.g., the Chief Information Security Officer (CISO)) and reporting structure, including the Cybersecurity Officer's independence and authority to make risk-based decisions and how the Officer reports to the Board. Additionally, provide information on cybersecurity resources, staff, and tools and how those are assessed against the cybersecurity strategy and any other programs of work to ensure alignment and appropriateness. Provide information on the budget process being consistent for all businesses and functions across the bank, including the cybersecurity program. For example, describe how software expenses, professional fees, etc. are included in the formal budget processes at both the global and country level. Describe the expenses approval process.	- Organizational structure, including designated persons, teams, organizations, and departments - Job Description/CV of CISO (or designated Cybersecurity Officer) - Engagement of consultants and professional services, as applicable - Board approvals - Related description of services provided by involved teams (e.g., service catalog) - Description of overall budget process, including cybersecurity	GV.RR-01	GV.RR-01.04

FS SSG.017	**Cybersecurity roles and responsibilities:** The roles, responsibilities, qualifications, and skill requirements for personnel (employees and third parties) that implement, manage, and oversee the technology, cybersecurity, and resilience programs are defined, aligned, coordinated, and holistically managed.	**1.A**	**Yes**	**Yes**	Organizational structure, roles, responsibilities, qualifications, and skill requirements, for levels of authority of the cybersecurity workforce should be clearly established and well-defined especially regarding roles required to handle sensitive data. The roles of personnel (employees and third parties) that implement and directly manage the technology, cybersecurity, and resilience programs are defined, aligned, coordinated, and holistically managed. A shared responsibilities model or similar mechanism should be established to ensure that all appropriate responsibilities are documented, managed, unambiguously assigned, and shared responsibilities are clear between a customer and third party service provider. Describe the roles and responsibilities throughout the cybersecurity workforce. Describe how management assesses whether the cybersecurity workforce has a reasonable and appropriate level of cybersecurity skills to perform their roles and responsibilities. Provide information related to the roles, responsibilities, and skillsets of personnel who directly manage and oversee the technology, cybersecurity, and resilience programs. Provide information on the role review process and frequency of review. Describe how profiles of specific roles are globally consistent and aligned across the organization.	- Organizational structure - IT security roles and responsibilities documents - Related training, certification, and skillset requirements - Related description of services provided by involved teams - Sample cybersecurity job descriptions/profiles - Workforce assessments (e.g., performance assessments) - Cybersecurity job profiles - Cyber resilience resourcing including threat analysis, security operations, and incident response - Risk appetite statements and risk metrics - Relevant Board or committee meeting agendas and minutes where roles and responsibilities or effectiveness are discussed - Third party contracts - Third party SSRM - Resource gap assessments	GV.RR-02	GV.RR-02.01
FS SSG.018	**Third-party risk management roles and responsibilities:** Roles and responsibilities for the Third-Party Risk Management Program and for each third-party engagement are defined and assigned.	--	--	**Yes**	All parts of the organization may be involved in third-party risk management (e.g., legal, IT, business management, etc.). As a result, the organization's management should ensure that roles and responsibilities are clearly defined and assigned for all aspects of the Third-Party Risk Management Program and for each third-party engagement including initiation of the relationship, ongoing oversight, and termination. Each third party relationship should have a defined responsible business manager assigned for effective oversight. Provide information on the roles and responsibilities for Third-Party Risk Management Program.	- Third-party security policy, standard, and procedures - Third-Party Risk Management Program - Documentation of roles and responsibilities for Third-Party Risk Management Program - Related reporting and examples - Designated third-party engagement managers	GV.RR-02	GV.RR-02.04
FS SSG.019	**Background checks:** The organization conducts (or causes the conduct of) background/screening checks on all personnel (employees and third party) upon hire/retention, at regular intervals throughout employment, and upon a change in role commensurate with their access to critical data and systems.	--	**Yes**	**Yes**	The organization should conduct background verifications for prospective employees and third parties with access to confidential or sensitive data, systems, or facilities. Furthermore, background checks should be conducted at regular intervals and upon change to the employee or third party's role. The organization may conduct background checks on third-party personnel directly or may employ contract clauses to ensure that background checks are performed by the third-party to approved standards. Background checks should be conducted in accordance with local laws, rules, and regulations. Describe how the organization conducts background/screening checks on all employees. If legal restrictions limit the scope of verification, then procedures should be defined consistent with the sensitivity of the data and processes being accessed, business requirements, or other legal considerations. Provide information on the governance and processes utilized for conducting background checks.	- Background/vetting/screening check policy, standards, and procedures - Metrics of operational effectiveness of policy, standards, and procedures - Standards or contract clauses for screening of third-party staff	GV.RR-04	GV.RR-04.01
FS SSG.020	**Employment termination:** The organization establishes processes and controls to mitigate cyber risks related to employment termination, as permitted by law, to include the return or disposition of all organizational assets.	**3.D**	**Yes**	**Yes**	Access management policies and procedures should establish a process for terminating users. If an organization terminates an individual's employment, there should be measures in place that require that user's access to any asset or system be removed immediately, including proprietary information (e.g., customer lists, etc.). The organization may put additional monitoring in place when an employee provides notice of termination (e.g., social media monitoring, data loss prevention, other security monitoring tools). Describe how the organization has established processes and controls to mitigate cyber risks related to employment termination, in consideration of legal restrictions, if any. Provide information on the termination process and related controls to include the return or disposition of all organizational assets.	- Access control policy and procedures covering employee termination - Termination/leave process to remove access when an employee terminates - Evidence of access removal within 24 hours of employee's departure - Evidence of monitoring activities (social media monitoring, data loss prevention, other security monitoring) - Method and/or process of reporting a violation - Investigations process - Evidence of return of assets	GV.RR-04	GV.RR-04.02

FS SSG.021	**Policy documentation and approval:** Technology and cybersecurity policies are documented, maintained and approved by the governing authority (e.g., the Board or one of its committees) or a designated executive.	**1.B**	**Yes**	**Yes**	The organization should have technology and cybersecurity policies, standards and procedures that align with risk and complexity and are approved by the governing authority (e.g., the Board or one of its committees) or a designated qualified executive. Generally, the technology and cybersecurity policies should include all operations and business processes supported by technology and define clear management accountability, to include responsibilities of staff that contribute to the development of the policies. The Board or one of its committees is responsible for overseeing the organization's technology and cybersecurity program, including reviewing and approving technology and cybersecurity policies. Provide information regarding the organizational structure for the management and operation of technology and cybersecurity enacted through policies and procedures, as well as governance forums for the management of controls. Describe how the Information Security Program is approved by the appropriate governing authority (e.g., Board Risk Committee) or designated executive. Describe how the Information Security Program is updated on a regular basis. Describe how technology and cybersecurity standards are defined by the cyber team and how the policies are regularly updated and reviewed by subject matter experts.	- Technology and Cybersecurity/Information Security Program documentation, including policy, methodology, charters for creating new policies, etc. - Catalog of approved or ratified policies, or description of which organization/business line within the organization owns and maintains each policy and who approved each policy - Policy roadmap or process document, including document control to determine if/when policies are reviewed and updated - Relevant Board and committee meeting agendas and minutes - Roles and responsibilities of 1LoD and 2LoD	GV.PO-01	GV.PO-01.01
FS SSG.022	**Incentive and accountability program alignment:** The organization's incentive programs are consistent with cyber risk management objectives, and technology and cybersecurity policies integrate with an employee accountability policy to ensure that all personnel are held accountable for complying with policies.	**--**	**Yes**	**Yes**	Management should implement incentive programs consistent with cyber risk management objectives to ensure employees know and understand their technology and cybersecurity responsibilities. Employees should provide explicit attestations indicating that they have read, understand, and agree to abide by the rules that describe their responsibilities and expected behavior regarding their technology and cybersecurity roles and responsibilities. For instance, employees may be required to review and signoff on technology and cybersecurity policies annually. Policies should also provide for disciplinary action if the employee fails to follow them. Provide information on assigned training (e.g., code of conduct including consequence management and mandatory training policy). In addition, provide any information and technology and cybersecurity policies that integrate with an employee accountability policy that may require assigned information and cybersecurity risk situational awareness training.	- Mandatory global risk objectives - Description of how employees include mandatory global risk objectives in personal performance scorecards - Technology and cybersecurity training curriculum - Technology and cybersecurity training for developers - Technology and cybersecurity situational awareness communications - Policy citations - Consequence models in place - Outcomes of assigned training, such as metrics of staff completed training to comply with requirements - Evidence of disciplinary action within policy and process for reporting policy violations, consistent with privacy regulations	GV.PO-01	GV.PO-01.03
FS SSG.023	**Physical and environmental security policies:** Physical and environmental security policies are implemented and managed.	**--**	**Yes**	**Yes**	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.	- Physical and environmental security policies (may also be called protective security policy), measures, and guidance - Standards, controls, and procedures supporting implementation of the policy into measurable objectives - Testing procedures to ensure physical controls are operating as expected (locked doors, server rack cabinets, badge readers, etc.) - Security logs, visitor access controls, or other measures that demonstrate compliance with policies - Workplace violence prevention policy	GV.PO-01	GV.PO-01.06

FS SSG.024	**Business continuity and resilience program policies:** The organization maintains documented business continuity and resilience program policies and procedures approved by the governing authority (e.g., the Board or one of its committees).	--	**Yes**	**Yes**	Provide information supporting the organization's business continuity and resilience program policies and procedures have been reviewed and approved by the governing authority (e.g., the Board or one of its committees). Business continuity and resilience program, policies, and procedures should be reviewed and approved regularly to ensure an organization can maintain, resume, and recover critical business functions and processes during and following an incident.	- Business continuity/resilience policy, standard, and procedures - Relevant Board and committee meeting minutes and approvals where business continuity and resilience program is discussed	GV.PO-01	GV.PO-01.07
FS SSG.025	**Third-party risk management policies:** The organization maintains documented third-party risk management program policies and procedures approved by the governing authority (e.g., the Board or one of its committees).	--	**Yes**	**Yes**	Provide information supporting the organization's third-party risk management policies and procedures have been reviewed and approved by the governing authority (e.g., the Board or one of its committees) and updated on a regularly basis. For example, policies may include a page indicating when it was last updated and who reviewed it. Describe how third-party risk management policies and procedures are regularly updates and reviewed by the governing authority.	- Third-party security policy, standard, and procedures - Third-party risk management program - Relevant Board or committee meeting minutes	GV.PO-01	GV.PO-01.08
FS SSG.026	**Policy review and update:** The cybersecurity policy is regularly reviewed, revised, and communicated under the leadership of a designated Cybersecurity Officer (e.g., CISO) to address changes in the risk profile and risk appetite, the evolving threat environment, and new technologies, products, services, and interdependencies.	**1.B**	**Yes**	**Yes**	The organization, under the leadership of the designated Cybersecurity Officer (e.g., CISO), should have a formal process that reviews and updates all cybersecurity-related policies across business lines periodically. Describe responsibility, process, and frequency for reviewing/revising policies. As new or enhanced cybersecurity regulations are published (trigger event(s)), new technologies, products, services become available or new cyber risks and threats are identified, show how policies are reviewed to ensure alignment or identify gaps (e.g., how trigger event(s) are consumed by the organization and updated in policies). Describe how the policy team communicates policy changes. Describe if annual training includes changes to policies.	- 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.PO-02	GV.PO-02.01
FS SSG.027	**Governing authority risk management review:** The governing authority (e.g., the Board or one of its committees) regularly reviews and evaluates the organization's ability to manage its technology, cybersecurity, third-party, and resilience risks.	--	--	**Yes**	The organization should have a process for evaluating changes to the organization's technology, cybersecurity, third-party, and resilience risks. The process should ensure that management updates the cyber risk management strategy, as needed, to effectively address emerging threats, vulnerabilities, and changes in risk internal and external to the organization. Provide information that demonstrates the appropriate governing authority reviews (scope, frequency, etc.) and evaluates the effectiveness with which the organization can manage its technology, cybersecurity, third-party, and resilience risks. Include examples of information provided to the governing authority.	- Relevant Board or committee (e.g., Board Risk Committee) meeting agendas and minutes - Risk and control reporting (e.g., risk maps, risk appetite reporting, risk and controls assessment reporting) - Target operating model (i.e., desired state of operations considering the organization's role in critical infrastructure)	GV.OV-01	GV.OV-01.01
IDENTIFY								
FS SSG.028	**Physical device asset inventory:** The organization maintains a current and complete asset inventory of physical devices, hardware, and information systems.	**2.A**	**Yes**	**Yes**	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.	- Asset management policies and procedures - Asset inventory documentation, including how often inventory is updated to maintain current data, how often it is reviewed and by whom (e.g., by independent risk management, audit), and the inventory method (e.g., automated, manual, or a combination) - Documentation supporting the operation, mapping, and discovery of assets - Asset related processes, roles, responsibilities, and evidence - Related dashboards, inclusive of KRIs / KPIs, on the efficiency and effectiveness of the asset management program - Related process flows	ID.AM-01	ID.AM-01.01

FS SSG.029	**Software and applications asset inventory:** The organization maintains a current and complete inventory of software platforms, business applications, and other software assets (e.g., virtual machines and virtual network devices).	**2.A**	**Yes**	**Yes**	An asset inventory is a comprehensive record of an organization's software platforms, business applications and other software (e.g., physical and virtual servers, operating systems, and business applications), and data repositories (e.g., customer information files or storage area network). The current inventory system of record is updated as frequently as necessary for the organization to successfully manage downstream processes reliant on an accurate asset inventory. However, management should update the asset inventory at least annually, or more frequently depending on risk, and should identify new assets as well as those relocated to another site. Describe the processes and tools related to maintaining a complete inventory of software platforms and business applications (refer to ID.AM-01.01 for asset inventory of physical devices, hardware, and information systems). The inventory should be integrated into the systems management lifecycle (through to destruction) and reconciled with other systems to ensure accuracy. The record will typically include the device type, and software version and end of support date to help the organization manage software updates, patches, and replacements. It will typically include the owner or responsible group, location/region, and the criticality or sensitivity level. It may also include the software utilized and data held at third parties. Firmware may be addressed as a component of this Diagnostic Statement or within the organization's set of configuration management controls.	- Asset management policies and procedures - Asset inventory documentation, including how often inventory is updated to maintain current data, and the inventory method (e.g., automated, manual) - Platform and application review process - Inventory issue resolution and attestation process documentation - Design governance documents - Related dashboards, inclusive of KRIs / KPIs, on the efficiency and effectiveness of the asset management program and related process flow diagrams - Asset related processes, roles, responsibilities, and evidence	ID.AM-02	ID.AM-02.01
FS SSG.030	**Network diagrams:** The organization maintains current maps of network resources, mobile resources, external connections, network-connected third parties, and network data flows.	**2.E**	**Yes**	**Yes**	To ensure appropriate network security, organizations should maintain accurate network and data flow diagrams that identify hardware, software, and network components, mobile components, internal and external connections, and types of information passed between systems to facilitate the development of a defense-in-depth security architecture. Management should be able to produce a visual depiction (e.g., diagram or topology map) of all external vendor or third-party connections. This could be a stand-alone document or part of the overall network topology. Provide information related to the organization's asset inventory that demonstrates the inventory includes maps of network resources as well as connections with external and mobile resources. A connection may be any internal or external connection. Examples include wireless, VPN, third-party service providers, network segments, or leased lines. Provide information on controls in place to ensure proper authentication and authorization to access organizational assets such as VPN devices, routers, external network resources, and wireless technologies.	- 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-03	ID.AM-03.01
FS SSG.031	**Third-party location asset inventory:** Hardware, software, and data assets maintained by or located at suppliers or other third parties are included in asset management inventories and lifecycle management processes as required for effective management and security.	--	--	**Yes**	Hardware, software, and data assets maintained by or located at suppliers or other third parties (e.g., remote access from personally owned devices, privately owned computing and communications devices, cloud services, etc.) are included in the organization's asset management inventory and lifecycle processes as required for effective management and security. Provide information related to the inventory that demonstrates the inventory includes the key characteristics of external information systems and who manages them (e.g., vendor, contractor, end user, etc.).	- Inventory reports which depict external information systems, their key characteristics, and who manages them - Policies and procedures for maintaining inventory of external hardware, software, and data assets - Diagrams or connectivity flow documentation - External systems point of contact information	ID.AM-04	ID.AM-04.01

FS SSG.032	**Asset protection prioritization:** The organization's hardware, software, and data assets are prioritized for protection based on their sensitivity, criticality, vulnerability, business value, and dependency role in the delivery of critical services.	--	--	**Yes**	As referenced in ID.AM-05.01, the organization implements and maintains a policy on data classification. Classification enables the organization to determine the sensitivity, criticality, vulnerability, business value, and dependency role of resources and prioritize assets accordingly to their classification. The asset priority will guide management's decisions regarding internal controls, and processes and security standards, and help assess controls applied by contracted third parties. Provide information on how critical assets are defined, classified, and prioritized (such as through a Business Impact Analysis). Describe the tools used to enable the organization to track, update, and provide custom reporting of the IT asset inventory (e.g., for vulnerability management, end-of-life/lifecycle management, business continuity plans, etc.).	- 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-05	ID.AM-05.02
FS SSG.033	**Data inventory:** The organization maintains a current inventory of the data being created, stored, or processed by its information assets and data flow diagrams depicting key internal and external data flows.	--	--	**Yes**	A data inventory is a comprehensive record of an organization's data repositories (e.g., customer information files or storage area network) as needed for effective management. A current inventory is updated as frequently as necessary for the organization to successfully manage downstream processes reliant on an accurate data inventory. However, management should update the asset inventory and its classifications at least annually, or more frequently depending on risk, and should identify new data classifications. Data classification is the identification and organization of information according to its criticality and sensitivity and usage. Describe the processes, tools, and data flow diagrams related to the inventory which includes types of data being created, stored, or processed by its information assets (e.g., cash positions, HR data, customer PII, trade data, post trade data, etc.). The organization should prioritize assets according to their classification in order to implement appropriate controls.	- Data management policies, procedures, and other documentation (e.g., data classification policy) - Operating guides - Data quality documentation - Data flow diagrams - Operating instructions - Related training for those modifying system of record - Related annual document review and approval	ID.AM-07	ID.AM-07.01
FS SSG.034	**Sensitive data physical protections:** The organization's asset management processes ensure the protection of sensitive data throughout removal, transfers, maintenance, end-of-life, and secure disposal or re-use.	--	--	**Yes**	An asset lifecycle is the sequence of stages that organizational assets go through during the time span of ownership. The organization should monitor and analyze the risks associated with the organization's assets through termination or disposal, with particular attention to protecting sensitive data through the asset's lifecycle. Provide information on the organization's asset management process. Describe how the assets are formally managed throughout removal, procurement, configuration, implementation into production, transfers, end-of-life, and secure disposal, or re-use of equipment processes, among other processes. Describe how data residing on the organization's assets is protected through the asset's lifecycle.	- Information asset security policy - Asset inventory - Secure disposal of electronic information policy, standard, and processes, which may include cryptographic destruction - Secure disposal of physical information policy, standard, and process - Evergreening policy, standard, and process - Mobile device management procedures for lost mobile devices	ID.AM-08	ID.AM-08.04
FS SSG.035	**Data destruction procedures:** The organization defines and implements standards and procedures, consistent with its data retention policy, for destroying or securely erasing data, media, and storage devices when the data is no longer needed.	--	--	**Yes**	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.	- Data retention policy, standard, and procedures - Data retention schedules - Data center data destruction procedures - Data destruction agreements with third parties, including attestation of data destruction	ID.AM-08	ID.AM-08.05

FS SSG.036	**Third-party data risk coverage:** Minimum cybersecurity requirements for third-parties cover the entire relationship lifecycle, from the acquisition of data through the return or destruction of data, to include limitations on data use, access, storage, and geographic location.	--	--	**Yes**	As referenced in EX.CN-02.01, the organization has documented minimum cybersecurity requirements for third parties. Describe how the minimum cybersecurity requirements for third parties cover the entire relationship lifecycle, including return or destruction of data, to include limitations on data use, access, storage, and geographic location. Management should consider including termination rights and recourse in contracts for a variety of conditions, including failure to meet cybersecurity requirements. Contracts should include provisions for timely return or destruction of the organization's data and resources. Include evidence from the third party documenting that data has been destroyed, such as an attestation or certification of destruction. In outsourcing to cloud service providers, the potential that data are not completely removed or deleted from the servicer's storage media at the conclusion of a service contract may pose higher risk in a cloud computing environment than in traditional outsourcing. It is important to ensure that the cloud service provider can remove confidential data from all locations upon termination of the relationship.	- 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	ID.AM-08	ID.AM-08.06
FS SSG.037	**Asset vulnerability identification:** The organization identifies, assesses, and documents risks and potential vulnerabilities associated with assets, to include workforce, data, technology, facilities, services, and connections.	--	--	**Yes**	Provide information on how the organization, at the enterprise and business unit (or lines of business) level, identifies, assesses, and documents risks and potential vulnerabilities. Describe how the organization's (lines of business) assessments of technology and cyber risks and vulnerabilities link to, or are associated with assets, workforce, data, technology, facilities, services, and connections. Reference current risk management frameworks and processes.	- Risk management frameworks and process documentation - Risk and control assessments and results - Various risk committee meeting agendas and minutes - Participation in cyber exercises, and related assessments of risks and vulnerabilities and action items	ID.RA-01	ID.RA-01.01
FS SSG.038	**Vulnerability management:** The organization establishes and maintains standards and capabilities for ongoing vulnerability management, including systematic scans, or reviews reasonably designed to identify known cyber vulnerabilities and upgrade opportunities, across the organization's environments and assets.	**2.B, 3.S**	**Yes**	**Yes**	Describe how the organization has established and maintains standards and capabilities for ongoing vulnerability management, including systematic scans or reviews reasonably designed to identify known cyber vulnerabilities. Describe how the organization determines eligibility and coverage for vulnerability scanning. Provide information on the processes and tools utilized to conduct systematic scans or reviews. Provide information on the assessment process after performing vulnerability management. Describe how the organization conducts ongoing vulnerability scanning, including automated scanning across the organization's environments and assets, to identify potential system vulnerabilities including known vulnerabilities, and upgrade opportunities. Provide information of strategy and scope. Provide information regarding the tools utilized. Describe any comparisons or reconciliations with asset inventories to ensure that all intended assets and environments are scanned.	- Vulnerability management security standards and procedures, including eligibility - Risk assessment criteria - Related tools - Applications and supporting infrastructure security testing policies, standards, and procedures - Related reporting (dashboards) - Remediation/patching processes - Evidence of asset reconciliation procedures to ensure comprehensive testing is completed against all environments - Risk acceptances for patches on systems, applications, etc. - Evidence of application security testing, including Web-based applications connected to the Internet, against known types of cyber attacks (e.g., SQL injection, cross-site scripting, buffer overflow) before implementation or following significant changes - Evidence of independent penetration testing of network boundary and critical Web-facing applications is performed routinely to identify security control gaps	ID.RA-01	ID.RA-01.03

FS SSG.039	**Threat identification and analysis:** The organization, on an ongoing basis, identifies, analyzes, correlates, characterizes, and reports threats that are internal and external to the firm.	--	--	**Yes**	The organization conducts a cyber threat analysis, on an ongoing basis, to identify cyber threats from internal and external sources that could materially affect its ability to perform or to provide services as expected. Threat intelligence gathering involves the acquisition and analysis of this information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance the organization's decision-making. The organization should establish an ongoing process to gather, analyze, correlate, characterize, and report relevant cyber threat information, including threats reported by third parties. Practices should be established for information sharing and reporting threats with third parties to understand both internal and external threats relevant to the firm. Describe the framework and processes used within the organization to identify, document, and analyze internal and external threats to the organization. Provide information regarding the threat intelligence structure and process.	- Cyber threat identification, documentation, analysis and response policies and procedures - Cyber threat intelligence and threat analysis reports - Cyber risk assessment documentation - Other related cyber threat assessments - Threat catalogs	ID.RA-03	ID.RA-03.01
FS SSG.040	**Stakeholder-provided threat information:** The organization solicits and considers threat intelligence received from the organization's stakeholders, service and utility providers, and other industry and security organizations.	--	--	**Yes**	Vulnerabilities and emerging threats are ever changing and increasing. Situational awareness is considered foundational to effective cybersecurity risk management. As a result, organizations should subscribe to information sharing resources that include threat and vulnerability information for situational awareness. Proactively sharing threat intelligence helps organizations achieve broader cybersecurity situational awareness among external stakeholders. Once validated, the organization's threat intelligence should be shared as appropriate. Describe how input from the organization's stakeholders, service and utility providers, and other industry and security organizations are reviewed, analyzed, aggregated, and considered as part of threat intelligence. Describe how customers, partners, researchers, or other external parties can report threats or suspected vulnerabilities to the organization.	- Cyber threat intelligence policies and standards - Vulnerability standards - Patch management policies and standards - Cyber threat intelligence reporting - Cyber incident reporting - Control environment meeting agendas and minutes - Risk assessment processes - List of staff and organization memberships - Threat catalog - Customer notifications about how to report suspected cyber issues	ID.RA-03	ID.RA-03.02
FS SSG.041	**Risk impact assessment:** The organization's risk assessment approach includes the analysis and characterization of the likelihood and potential business impact of identified risks being realized.	--	--	**Yes**	Cyber risks can lead to financial, strategic, regulatory, and compliance impacts. For example, a data breach can result in customer notification and credit monitoring costs, as well as reputational damage and regulatory fines. The organization should track the financial impact cyber incidents may have on the organization's capital. Analyzing the financial impact associated with cybersecurity incidents helps an organization align and prioritize resources to risks with greater financial impacts. Provide information on how the risk assessment approach includes the identification of the likelihood and potential business impact of cyber risks.	- Business impact assessments - Risk assessment methodology - Operational risk management framework - Risk and control assessments - Application security reviews - Third-party security reviews - Independent risk and residual risk likelihood and impact reports	ID.RA-04	ID.RA-04.01
FS SSG.042	**Risk assessment considerations:** Threats, vulnerabilities, likelihoods, and impacts are used to determine overall technology, cybersecurity, and resilience risk to the organization.	--	--	**Yes**	The organization's risk assessment methodology should include the analysis of threats, vulnerabilities, likelihoods, and impacts in the determination and characterization of risks to the organization. Threat intelligence gathering and assessment involves the acquisition and analysis of this information to identify, track, and predict cyber capabilities, intentions, and activities of malicious actors and can inform the overall technology, cybersecurity, and resilience risk to the organization. Integration and analysis of threat intelligence should inform the organization's decision-making regarding technology, cybersecurity, and resilience risk reduction activities. Provide information showing threat, vulnerability, likelihood, and impact assessments are linked to the overall evaluation of technology, cybersecurity, and resilience risk to the organization.	- Operational risk framework - Risk reporting - Overall assessments of cyber risk to the organization - Impact assessments - Risk assessment methodology - Enterprise risk strategy - Subscription to threat intelligence feeds that inform the organization of changing threat condition over time	ID.RA-05	ID.RA-05.01

FS SSG.043	**Scenario planning and table-top-exercises:** The organization uses scenario planning, table-top-exercises, or similar event analysis techniques to identify vulnerabilities and determine potential impacts to critical infrastructure, technology, and business processes.	**2.C**	**Yes**	**Yes**	Describe how the organization uses scenario planning, table-top-exercises, or similar event analysis techniques to identify vulnerabilities and determine potential impacts to critical infrastructure, technology, and business processes. For example, scenarios may include cyber events demonstrating the ability of the organization, as well as its third-party providers, to respond quickly and efficiently to a cyber incident, such as a DDoS attack. Tabletop exercises may also identify critical single points of failure in staff or other resources. Provide information on how organizations address potential single points of failure.	- Security incident response policies, standards, and procedures - Tabletop exercises and/or simulations - Use cases - Related assessment reporting - List of applicable use cases or scenarios for test cases	ID.RA-05	ID.RA-05.04
FS SSG.044	**Prioritization of risk remediation responses:** The implementation of responses to address identified risks (i.e., risk avoidance, risk mitigation, risk acceptance, or risk transfer (e.g., cyber insurance)) are formulated, assessed, documented, and prioritized based on criticality to the business.	--	--	**Yes**	Responses should provide various methods for risk response, including risk avoidance, risk mitigation, risk acceptance, or risk transfer, based on the potential impact to the delivery of critical services and criticality to the business. The organization documents, assesses, formulates, and prioritizes identified risks to determine the appropriate response approach. Organizations use their risk management framework and processes to prioritize the implementation of responses. Describe the processes and tools used to address identified cyber risks. Include information on the processes used for risk acceptance, risk mitigation, risk avoidance, or risk transfer, which includes cyber insurance. Provide examples supporting how a risk is mitigated (e.g., implementing new controls), justification if a risk is accepted, etc. Describe the role of various stakeholders in the formulation and prioritization of risk responses.	- Risk acceptance and risk exception procedures - Risk management framework - Reviews demonstrating risk acceptance standard is followed (e.g., application and system security reviews, security testing standard for applications and infrastructure, etc.) - Cyber and business insurance documentation - Risk assessment methodology - Communications regarding issues and findings between cyber risk identification and remediation teams - Remediation activity logs	ID.RA-06	ID.RA-06.02
FS SSG.045	**Prioritization of vulnerability remediation:** The organization defines and implements standards and procedures to prioritize and remediate issues identified in vulnerability scanning or penetration testing, including emergency or zero-day threats and vulnerabilities.	--	**Yes**	**Yes**	Vulnerability management is a key control to ensure known vulnerabilities in systems, applications, and devices are uncovered before they are placed into production. Vulnerability scanning and/or penetration testing is normally conducted on a routine basis, as well as during systems development lifecycle, and acquisition activities. Provide information on metrics and reporting used to prioritize and remediate issues identified. Describe what standards, procedures, and processes the organization has established to prioritize and remedy issues identified through vulnerability scanning and penetration testing. Issues identified should integrate patching processes, standards, and procedures in place. Describe the prioritization methodology, such as potential impact, time to remedy, etc., and the process for vulnerability scanning and penetration testing. Provide information of any exception procedures employed.	- Vulnerability management security standards and processes - Remediation/patching processes - Metrics and reporting used - Exception management processes - Remediation reports or metrics with timelines - Risk acceptances for patches on systems, applications, etc. - Related reporting (dashboards)	ID.RA-06	ID.RA-06.05
FS SSG.046	**Change management standards and procedures:** The organization defines and implements change management standards and procedures, to include emergency change procedures, that explicitly address risk identified both prior to and during a change, any new risk created post-change, as well as the reviewing and approving authorities (e.g., change advisory boards).	**3.N**	**Yes**	**Yes**	Change management involves a policy, procedures, and standards that guide a broad range of changes within an organization's operating environment. Changes may include configuration changes, such as security settings, hardware changes that address obsolescence, routine software releases, including those provided by a third party, or emergency fixes and patches that eliminate software or other vulnerabilities. Technology projects and system implementations may also introduce a broad range of changes, both technical and business-related, which should be managed effectively. To ensure risks and vulnerabilities are not introduced with changes, the change management process needs to include a security impact, business impact, or similar analysis. Describe how the organization's change management process explicitly considers risks, in terms of residual risks identified both prior to and during a change, and of any new risk created post-change. Describe how pre- and post-change testing, and back-out plans, are integrated into the procedures. Describe how emergency changes may be handled differently than routine or standard changes. Provide information related to the change management process, and approval authorities (e.g., change advisory boards).	- Secure system development standard - Security testing standard for applications and supporting infrastructure - Change management policy, standard, and process, including: - Risk evaluation - Formal approval processes - Implementation and backout test plans - Control indicator reporting - Change advisory boards meeting minutes - Related documentation (e.g., possibly change tickets) - Project management standards and procedures	ID.RA-07	ID.RA-07.01

FS SSG.047	**Risk exception management:** Policy exceptions, risk mitigation plans, and risk acceptances resulting from assessments and evaluations, such as testing, exercises, audits, etc., are formally managed, approved, escalated to defined levels of management, and tracked to closure.	**3.M**	**Yes**	**Yes**	Responses should provide risk management strategies, procedures, standards, and policies that are inclusive of policy exceptions, risk mitigation plans, and risk acceptances. Describe tracking of status on risks identified from testing, exercises, audits, etc. and the number/types of reports, including any dashboard which provide details on risks and threats identified, mitigating actions proposed and their status tracked until closure. Provide information on the organization's formal exception management process for risks that cannot be mitigated. Describe the process of escalation of policy exceptions to defined levels of management, review/ongoing monitoring, and approval. Responses should provide evidence on an approved risk response prior to formal closure of any assessment and evaluation issue identified. Where risks may be accepted, identify any standards for re-review of the exception at regular intervals.	- Risk acceptance policy, standard, and procedures - Risk acceptance/exception management process - Required approvals - Evidence of mitigation (e.g., follow-up reports, routine reviews, updates) - Cyber-related reviews demonstrating risk acceptance standard is followed (e.g., application and system security reviews, security testing standard for applications and infrastructure, etc.) - Risk management framework - Cyber risk assessment methodology - Audit issue tracking reports and escalation criteria - Evidence of risk exceptions to applicable policies	ID.RA-07	ID.RA-07.04
FS SSG.048	**Vulnerability exception management:** The organization establishes and maintains an exception management process for identified vulnerabilities that cannot be mitigated within target timeframes.	**2.B**	**Yes**	**Yes**	Exception management processes should specifically address vulnerabilities that cannot be mitigated due to unsupported or end-of-life hardware, software, or applications. Provide information on the organization's exception management process for vulnerabilities that cannot be mitigated due to business-related exceptions. Describe the process of review and approval and ongoing monitoring/reporting of exceptions.	- Risk acceptance/exception management process - Required approvals - Risk acceptances for delay to patches on systems, applications, etc. - Documentation of any network segmentations and VLANS - Related reporting (dashboards) - RACI matrix for exception management - Standards and procedures for the management of unsupported or end-of-life systems	ID.RA-07	ID.RA-07.05
FS SSG.049	**Vulnerability disclosure receipt:** The organization has established enterprise processes for soliciting, receiving and appropriately channeling vulnerability disclosures from: (1) Public sources (e.g., customers and security researchers); (2) Vulnerability sharing forums (e.g., FS-ISAC); and (3) Third-parties (e.g., cloud vendors); (4) Internal sources (e.g., development teams).	**2.D**	**Yes**	**Yes**	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.	- Vulnerability management security standard - Cyber threat reporting and intelligence examples - Cyber threat analysis examples - Organizational structure - Related description of services provided by involved teams - Related job profiles - Group distribution lists - Related collaboration and information sharing examples - Contractual information sharing agreements	ID.RA-08	ID.RA-08.01
FS SSG.050	**Control testing:** Technology, cybersecurity, and resilience controls are regularly assessed and/or tested for design and operating effectiveness.	--	**Yes**	**Yes**	Technology, cybersecurity, and resilience controls should be tested regularly to validate the design and operating effectiveness of the controls. Describe the process for ensuring controls are implemented and developed correctly and are operating as intended. Describe how the controls testing program integrates with risk assessment, exception management, and controls program assessment processes. Provide information of testing and assessments performed to identify weaknesses and deficiencies in the control design and development process to identify areas that need improvement.	- Applicable assessment results - Testing procedures to ensure technology, cybersecurity, and resilience controls are operating as expected - Evidence of testing performed routinely to identify security control gaps	ID.IM-01	ID.IM-01.01

FS SSG.051	**Key indicators and risk metrics:** The organization implements a regular process to collect, store, report, benchmark, and assess trends in actionable performance indicators and risk metrics (e.g., threat KRIs, security incident metrics, vulnerability metrics, and operational measures).	--	--	**Yes**	The organization should establish a risk and operational baseline and set benchmarks or target actionable performance indicators and risk metrics. A methodology should be implemented to determine if the organization is failing to meet, meeting, or exceeding those established benchmarks. Provide information on the effectiveness of controls measured through a suite of KCI, KPI, and/or KRI that were defined and mapped to controls or operational activities. Additionally, describe the KCI/KPI/KRI formal review process and roles and needs of the various stakeholders for the reporting. Describe consistency with KCIs/KPIs/KRIs reporting across local/global business lines' countries and/or regions which are for use in governance forums. Also provide information on how control owners (or others) assess maturity (e.g., on a scale 1-5) of controls and operational processes and the linkage to any improvement programs to uplift maturity. Define how and who independently validates the assessments.	- KCI/KPI/KRI dashboards - Risk appetite statement, which may include metrics or other measures (e.g., reporting documents/dashboards) - Relevant Board or committee meeting agendas and minutes - Process for modifying/maintaining KCIs/KPIs/KRIs - Maturity model or methodology used to align KPIs and metrics	ID.IM-01	ID.IM-01.02
FS SSG.052	**Penetration testing:** The organization conducts regular, independent penetration testing and red team testing on the organization's network, internet-facing systems, critical applications, and associated controls to identify gaps in cybersecurity defenses.	**2.C**	**Yes**	**Yes**	Penetration testing attempts to exploit potential vulnerabilities to determine whether unauthorized access or other malicious activity is possible. The organization or an independent third-party (e.g., qualified independent contractor, internal audit) should perform penetration testing and/or red team testing (or equivalent) on the organization's network, internet-facing applications or systems, and other critical applications on existing components of the network, as well as the external network and environment. Testing may be extended on associated controls, such as physical access management. Describe how the organization conducts periodic penetration testing and red team testing (commensurate with the nature of the threats to the organization and its assets) on the internal and external network, environment, internet-facing applications or systems, and critical applications to identify gaps in cybersecurity defenses. If an independent third-party is used, provide information on the use and scope of the third-party testing.	- Security testing for applications and supporting infrastructure policies, standards, and procedures - Vulnerability management security policies, standards, and procedures - Proof that penetration testing tools and processes are independent and conducted according to the risk assessment for external facing systems - Red team tools and processes - Copy of penetration tests along with remediation plans - Related reporting (e.g., issues, lessons learned, final report, etc.) - Proof that testing is conducted at least annually and based upon changes to the environment and risk identification	ID.IM-02	ID.IM-02.01
FS SSG.053	**Resilience strategy and plan testing:** The organization's testing program validates the effectiveness of its resilience strategy and response, disaster recovery, and resumption plans on a regular basis or upon major changes to business or system functions, and includes external stakeholders as required.	**1.C**	**Yes**	**Yes**	Describe how the organization promotes, designs, organizes, and manages testing exercises that are designed to test its resilience strategy and response, disaster recovery, and resumption plans, with participation from internal and external stakeholders as required, on a regular basis or upon major changes to business or system functions. Include information on how the organization shares results of testing exercises to the appropriate parties through metrics or board reporting. Describe how the organization's testing program validates the effectiveness of its resilience strategy, response, disaster recovery, and resumption plans on an annual or more frequent basis according to major changes to business or system functions and the risk profile of the organization. Provide information on the organization's testing framework and strategy. Describe the types of testing performed. As referenced in ID.IM-02.05, the organization establishes testing programs should include a range of scenarios.	- Business continuity/resiliency plans, policies and procedures - Network penetration testing strategy - Application security testing strategy - Data recovery testing - Targeted test results and reports - Security assessments - Results of testing exercises, including metrics or board reporting - Evidence of testing critical online systems and processes to withstand stresses for extended periods (e.g., DDoS) - Evidence that testing involves collaboration with critical third parties - Evidence that testing is comprehensive and coordinated across all critical business functions - Evidence of all tests conducted in the past 12 months for business continuity / disaster recovery	ID.IM-02	ID.IM-02.04

FS SSG.054	**Resilience testing scenarios:** The organization establishes testing programs that include a range of scenarios, including severe but plausible scenarios (e.g., disruptive, destructive, corruptive), that could affect the organization's ability to service internal and external stakeholders.	**1.C**	**Yes**	**Yes**	Describe how the organization establishes testing programs based on the risk profile of the organization business impact analyses, and resilience risk analyses. Describe how the testing programs include a range of scenarios, including severe but plausible scenarios (e.g., disruptive, destructive, corruptive) that could affect the organization's ability to service internal and external stakeholders. These scenarios should have a range of cyber, environmental, third-party, and business scenarios.	- Business continuity/resiliency plans, policies, and procedures - Roles and responsibilities for staff involved in resumption of critical operations - Evidence of tabletop exercises or other testing programs - Business continuity / disaster recovery exercises that were conducted in the past 12 months - List of applicable use cases or scenarios for test cases - Business impact analysis and business continuity management risk analyses - Internal and external dependency analyses	ID.IM-02	ID.IM-02.05
FS SSG.055	**Accurate data recovery:** The organization designs and tests its systems and processes, and employs third-party support resources (e.g., Sheltered Harbor), to enable recovery of accurate data (e.g., material financial transactions) sufficient to support defined business recovery time and recovery point objectives.	**3.O**	**Yes**	**Yes**	Describe how the organization designs and tests its systems and processes, and employs third-party support resources to enable recovery of data (e.g., material financial transactions) sufficient to support defined business recovery time and recovery point objectives. For example, an organization can use Sheltered Harbor for third party support to securely store and quickly restore data and services to meet business recovery time and recovery point objectives. Describe how the organization designs requirements for backups and replications of data based on data sensitivity and criticality. Describe how the organization employs third party support resources to enable recovery of accurate data. Provide information regarding systems and processes risk classification as it pertains to design and testing frequency. Provide information on the types of backups utilized based upon the risk classification.	- Business continuity/resiliency plans - Risk management frameworks and process documentation considering likely recovery scenarios and impact to data integrity, data loss and availability - Information classification - Service continuity planning policy, standards, and processes - Related testing results and reports - Incident response plan - Articulation of participation in industry-wide back-up methodologies such as the Sheltered Harbor program within the FS-ISAC	ID.IM-02	ID.IM-02.06
FS SSG.056	**Alignment of business continuity, disaster recovery, and response programs:** The organization's business continuity, disaster recovery, crisis management, and response plans are in place and managed, aligned with each other, and incorporate considerations of cyber incidents.	**1.C**	**Yes**	**Yes**	The organization should have approved business continuity, disaster recovery, crisis management, and response plans in place to recover operations following an incident. The organization should have plans in place that address business impact analysis and risk assessment, alternate processing for critical business functions while systems/applications and facilities are unavailable. The organization should establish recovery strategies and procedures for critical systems, roles and responsibilities, and business continuity and disaster recovery testing that are managed and aligned with each other. Plans should be integrated and aligned to prepare an organization to continue critical business services during disruption. Describe how the organization's business continuity (business process), disaster recovery (data center process), crisis management (business process), and incident response plans (incident process) are in place, coordinated, managed, aligned with each other, and incorporate considerations of cyber incidents.	- Policies, standards, plans, and procedures that relate to business continuity, resiliency, disaster recovery planning, crisis management, and incident response - Recent business impact analysis - Organizational information - List of essential staff members, including roles and responsibilities - Related tabletop exercises - Stress tests of infrastructure and services - Run books for business continuity / disaster recovery	ID.IM-04	ID.IM-04.01
FS SSG.057	**Incident management roles and responsibilities:** The organization's incident response and business continuity plans contain clearly defined roles, responsibilities, and levels of decision-making authority, and include all needed areas of participation and expertise across the organization and key third-parties.	--	--	**Yes**	Describe how the organization's incident response plan and business continuity plans contain clearly defined roles, responsibilities, and levels of decision-making authority. The organization may use RACI charts to define leadership, ownership, and accountability of specific roles and responsibilities to ensure all needed areas of participation and expertise are included from internal and external stakeholders. The organization's incident response plan and business continuity plan should include details on decision making authority and escalation procedures.	- Security incident response policies, standards, and procedures - Responsibility assignments chart (e.g., RACI charts) including key roles such as team lead, communications lead, legal representative, etc. - Business continuity/resilience policy, standard, and procedures	ID.IM-04	ID.IM-04.02

FS SSG.058	**Incident management support resources:** The organization pre-identifies, pre-qualifies, and retains third party incident management support and forensic service firms, as required, that can be called upon to quickly assist with incident response, investigation, and recovery.	--	--	**Yes**	Describe processes for an organization pre-identifying, pre-qualifying, and retaining third party support to effectively prepare and respond to an incident in a timely manner. Organizations should develop and prepare for potential incidents by developing an incident response management plan that is periodically tested (e.g., scenario planning, tabletops, etc.) with the participation of third parties. Response roles and responsibilities should be defined for internal and external individuals to ensure an organization is able to quickly and effectively assist with incident response, forensic, investigation, and recovery.	- Security incident response policies, standards, and procedures - Roles and responsibilities (i.e., forensics, root cause analysis teams) - Contracts or retainer agreements for forensic investigation expertise	ID.IM-04	ID.IM-04.07
FS SSG.059	**Response program improvement:** The organization regularly reviews response strategy, incident management plans, recovery plans, and associated tests and exercises and updates them, as necessary, based on: (1) Lessons learned from incidents that have occurred (both internal and external to the organization); (2) Current cyber threat intelligence (both internal and external sources); (3) Recent and wide-scale cyber attack scenarios; (4) Operationally and technically plausible future cyber attacks; (5) Organizational or technical environment changes; and, (6) New technological developments.	**1.C, 6.A**	**Yes**	**Yes**	Describe how the organization periodically reviews response strategy, incident management plans, recovery plans, and associated test and exercises and updates them as necessary based on the six criteria within the statement (lessons learned, cyber threat intelligence, recent cyber-attacks, future cyber-attacks, environment changes, and new technology).	- Security incident response policy, standard, and procedures - Incident response examples or playbooks - Cyber analysis and reporting - Related standards and processes	ID.IM-04	ID.IM-04.08

	PROTECT							
FS SSG.060	**Identity and credential management:** Identities and credentials are actively managed or automated for authorized devices and users (e.g., removal of default and factory passwords, password strength requirements, automatic revocation of credentials under defined conditions, regular asset owner access review, etc.).	**3.A, 3.B, 3.C**	**Yes**	**Yes**	The goal of access control is to allow access by authorized individuals and devices and to disallow access by all others. Role-based access control may be considered to simplify management activities. Access should be authorized and provided only to individuals whose identity is established, and their activities should be limited to the minimum required for business purposes. Asset owners should regularly review access roles and individuals authorized to access the system to verify appropriate access management procedures. Access controls should include password complexity, limitation of the number of password attempts before a user is locked out, and prohibition of the reuse of passwords. The organization should create complex passwords for default administration passwords, otherwise the network may be vulnerable to attack or employee abuse. Default passwords should be changed per system implementation guidelines, change management procedures or system hardening documentation. Changes to access privileges of critical systems should be continuously monitored and any changes to those access privileges should result in an alert and notification to the proper security team to investigate, document, and resolve any issues. Where possible, access management activities should be automated to reduce error and manual processing overhead. Access management policies and procedures should establish a process for terminating users. If an organization terminates an individual's employment, there should be measures in place that require that user's access to any asset or system be removed immediately. Provide information in support of identities and credentials being actively managed and/or automated for authorized devices and users.	- Access control policy and related procedures - Role-based access control standard and procedures - Password/pin management standard - Access request process - Risk-based periodic access review - Other assessments of applications or systems validating compliance with access control policy and related procedures, such as use of password vaulting applications to control privileged credentials	PR.AA-01	PR.AA-01.01
FS SSG.061	**Physical and logical access:** Physical and logical access to systems is permitted only for individuals who have a legitimate business requirement, have been authorized, and who are adequately trained and monitored.	--	**Yes**	**Yes**	The organization's management should ensure all users are identified and authenticated when accessing systems, applications, and hardware. Asset owners should determine the appropriate persons to allow access to and the types of access roles in place at the organization. Provide information regarding the physical and logical access controls that demonstrate that access is only permitted to individuals who have a legitimate business requirement, have been authorized, and who are adequately trained and monitored. Describe the request and review process and how that supports the statement. Describe the training and monitoring conducted for users, particularly those with access to sensitive and/or critical data.	- Access control, request, and review security standards and policy - Physical security assessment results and other related reports - Physical access logs and entrance approval lists - Access approval document (monthly, quarterly, annually) - Entitlement review reports - Physical access controls for network ports, collaborative computing devices, and applications - Related training	PR.AA-01	PR.AA-01.02
FS SSG.062	**Authentication of identity:** The organization authenticates identity, validates the authorization level of a user before granting access to its systems, limits the use of an account to a single individual, and attributes activities to the user in logs and transactions.	**3.C**	**Yes**	**Yes**	The organization's management should ensure all users are identified and authenticated when accessing systems, applications, and hardware. Identification of a user is commonly associated with a user account name or other identifier, such as a unique identifier, account number, or email address. Provide information on how the organization authenticates identity, validates the authorization level of a user before granting access to its systems, limits the use of an account to a single individual, and attributes activities to the user in logs and transactions. Provide information on authentication methods (e.g., MFA) determined by the risk of the user and/or transaction type. Describe how the organization attributes activities to the user in logs and transactions. For example, a process in place to record the ID of the user performing a transaction in all logs and application records to accurately recreate the activity.	- Identity access management policy, standards, and procedures - Identification and authentication policy, standards, and procedures - Network access control standards and procedures - Access request and review security standard and procedures - Access control security standard - Password/PIN management standards - Role based access control documentation - Sample requests - Call center authentication procedures	PR.AA-02	PR.AA-02.01

FS SSG.063	**Authentication requirements:** Based on the risk level of a user access or a specific transaction, the organization defines and implements authentication requirements, which may include multi-factor or out-of-band authentication, and may adopt other real-time risk prevention or mitigation tactics.	**3.E, 3.F**	**Yes**	**Yes**	The organization should conduct risk assessments and use effective authentication methods appropriate to the level of risk of a given transaction, user access, or connection. Best practices include: selecting authentication mechanisms based on the risk associated with the particular application or service; considering whether multi-factor authentication is appropriate for each application; and encrypting the transmission and storage of authenticators (e.g., passwords, personal identification numbers (PINs), digital certificates, and biometric templates). Describe how, based on the risk level of a given transaction, user access, or connection, the organization has defined and implemented appropriate authentication requirements.	- Authentication security policy, standard, and procedures - Identification and authentication policy, standards, and procedures - Service level management standard - Privileged access policy, standard, and procedures - Third-party access policy, standard, and procedures - Real-time risk prevention or mitigation tactics - Application/service access risk assessment	PR.AA-03	PR.AA-03.01
FS SSG.064	**Email verification mechanisms:** The organization reduces fraudulent activity and protects reputational integrity through email verification mechanisms (e.g., DMARC, DKIM), call-back verification, secure file exchange facilities, out-of-band communications, customer outreach and education, and other tactics designed to thwart imposters and fraudsters.	**3.L**	**Yes**	**Yes**	Address spoofing, phishing, and man-in-the-middle attacks are common email exploits that can damage the reputational integrity of an organization. Responses should include an organization's email verification mechanisms such as Domain-based Message Authentication, Reporting, and Conformance (DMARC), Domain Keys Identified Mail (DKIM), call-back verification, secure file exchange facilities, out-of-band communications, customer outreach and education, or similar authentication protocol mechanisms implemented to protect email confidentiality and reputational integrity. Describe which email verification mechanisms have been implemented to reduce fraudulent activity and thwart imposters and fraudsters. Provide information on the mechanisms utilized.	- Proof that email protection mechanisms are used to filter for common cyber threats (e.g., attached malware or malicious links) - Managing electronic information policies, standards, procedures - Email server security standards	PR.AA-03	PR.AA-03.03
FS SSG.065	**Access control within and across security perimeters:** Access credential and authorization mechanisms for internal systems and across security perimeters (e.g., leveraging directory services, directory synchronization, single sign-on, federated access, credential mapping, etc.) are designed to maintain security, integrity, and authenticity.	**--**	**Yes**	**Yes**	As referenced in PR.AA. Responses should ensure that authorized personnel have credentials and authentication mechanisms in place for physical and logical access, specific to their job duties, and while implementing least privilege access for internal systems and across security perimeters. Authorization mechanisms should be in place to centralize access control including directory services, directory synchronization, single sign-on, federated access, credential mapping, etc.). Refer to DE.CM-06.01, the organization should have processes to review, document, and authorize, all third-party connections, data transfer mechanisms, and Application Programming Interfaces (APIs). Describe authorization mechanisms that are implemented and designed to maintain security, integrity, and authenticity.	- Access request process - Risk-based periodic access review - Computer system access control policy, standard, and procedures - Inventory and ownership of service accounts - Periodic review of access authorization documentation and password refresh - Proof that authorization mechanisms are implemented for internal systems and across security perimeters - Third party connection authorization documentation	PR.AA-04	PR.AA-04.01
FS SSG.066	**Access privilege limitation:** The organization limits access privileges to the minimum necessary and with consideration of separation of duties (e.g., through role-based access control, asset owner access recertifications, etc.).	**3.H**	**Yes**	**Yes**	Least privilege refers to allowing only authorized access for users which are necessary to accomplish the assigned tasks in accordance with organizational missions and business functions. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. The organization should limit access privileges with consideration of separation of duties by only granting access needed to perform an individual's role and responsibilities. Responses should ensure that authorized personnel have credentials and authentication mechanisms in place for physical and logical access, specific to their job duties, and while implementing least privilege access for internal systems and across security perimeters. Authorization mechanisms should be in place to centralize access control including directory services, directory synchronization, single sign-on, federated access, credential mapping, etc.) Describe authorization mechanisms that are implemented and designed to maintain security, integrity, and authenticity. Provide information regarding how the organization limits access privileges to the minimum necessary and with consideration of separation of duties.	- 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.AA-05	PR.AA-05.01

FS SSG.067	**Privileged system access:** The organization institutes controls over privileged system access by strictly limiting and closely managing staff and services with elevated system entitlements (e.g., multi-factor authentication, dual accounts, privilege and time constraints, etc.)	**3.F, 3.G**	**Yes**	**Yes**	The organization should provide the necessary reviews and authorization (approval) for privileged access when necessary. Good practices for controlling privileged access include: identifying each privilege associated with each system component, implementing a process to allocate privileges and allocating those privileges either on a need-to-use or an event-by-event basis, documenting the granting and administrative limits on privileges, and finding alternate ways of achieving the business objectives, among other practices. Management should implement database access controls that help prevent unauthorized download or transmission of confidential data. Managers of persons with privileged access should understand the nature of the access required and be able to identify appropriate and inappropriate activity. Provide information on how the organization institutes controls over privileged system access by strictly limiting and closely managing staff and services with elevated system access entitlements. Describe the risk-based approach and frameworks in place.	- Privileged access policy, standard, and procedure - Committee meeting agendas and minutes supporting the topic - Privileged account management system documentation and procedures - Privileged account monitoring and alerting procedures - Periodic review of access authorization documentation - Evidence that administrators have two accounts; one for administrative use and one for general purpose - Evidence of controls to prevent unauthorized escalation of user privileges such as software installation	PR.AA-05	PR.AA-05.02
FS SSG.068	**Service accounts:** 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.	**3.C**	**Yes**	**Yes**	The organization should develop security standards based on industry configuration guidelines that establish specific baseline security controls. Provide information on how the organization institutes controls over service accounts, including third party connections. Refer to DE.CM-06.01, for how the organization should authorize third party connections. Provide information on the lifecycle framework in place to ensure strict security over creation, use, and termination of access credentials, reviews of account ownership, visibility for authorized use, and hardening against malicious insider use. For example, when service accounts are retired, the associated credentials should also be returned. If not controlled and restricted to authorized users, service accounts may impact network performance and disable key controls.	- Computer system access control policy, standard, and procedures - Access request and review security standard - System hardening standards - Application whitelisting tools and procedures - Privileged access policy, standard, and procedure - Service account policy - Inventory and ownership of service accounts - Periodic review of access authorization documentation and password refresh - Third party connection authorization documentation	PR.AA-05	PR.AA-05.03
FS SSG.069	**Third-party access management:** Specific roles, responsibilities, and procedures to manage the risk of third-party access to organizational systems and facilities are defined and implemented.	--	--	**Yes**	A third-party security policy or vendor management policy may assign specific roles and responsibilities to manage the risk of third-party access to the organization's system and facilities. Describe how specific roles, responsibilities, and procedures for third-party risk management are defined and implemented by the organization. As needed, restrictions or controls for third-party access to systems (i.e., for individuals and service accounts) are addressed in contracts and agreements.	- Third-party security policy, standard, and procedures - Third-party risk management program - Documentation of roles and responsibilities for external dependencies - Documentation on contract language that permits monitoring of third-party access - Related reporting and examples	PR.AA-05	PR.AA-05.04
FS SSG.070	**Physical access security:** The organization manages, protects, and logs physical access to sensitive areas, devices, consoles, equipment, and network cabling and infrastructure.	--	**Yes**	**Yes**	The organization should log and monitor the physical environment (e.g., entrances, restricted areas, confidential data repositories, vault areas, and ATMs) to prevent unauthorized access attempts and enable response efforts. Implementing appropriate preventative and detective physical controls protects systems, data, employees, and infrastructure against malicious or unauthorized persons. Sessions on systems and applications that handle sensitive customer data should have controls in place to lock or close the session and require users to re-authenticate (e.g., security settings or parameters for inactivity in Windows Active Directory and the core processing system). Describe how the organization manages, protects, and logs physical access to sensitive areas, devices, consoles, equipment, and network cabling and infrastructure.	- Physical access controls policy - Related logs - Sensitive area access process documentation - Physical security access recertification documentation - Access request and review security standard - Use of equipment and systems documentation - Protection of off-premises equipment documentation (e.g., full disk encryption for laptops or thumb drives)	PR.AA-06	PR.AA-06.01

FS SSG.071	**Physical and visual access to information assets:** The organization manages and protects physical and visual access to sensitive information assets and physical records (e.g., session lockout, clean desk policies, printer/facsimile output trays, file cabinet/room security, document labelling, etc.)	--	--	**Yes**	Provide information on physical and visual access controls implemented according to the assets at risk (e.g., data, infrastructure, systems). Responses should have physical and environmental policies, standards, and procedures in place that are aligned to the organization's risk management strategy and framework. Describe how the organization develops and manages individuals with authorized access to the organization's facilities. Describe how the organization issues credentials for facility access, disables sessions after an established period of inactivity (e.g., session lockout), and monitors physical access. Training materials should be employed to ensure personnel are informed of clean desk policies, file cabinet/room security, document labelling, and printer/facsimile output tray procedures.	- Physical access controls policy - Security logs, visitor access controls, or other measures that demonstrate compliance with policies - Sensitive area access process documentation - Physical security access recertification documentation - Access request and review security standard - Use of equipment and systems documentation - Related training - Protection of off-premises equipment documentation (e.g., full disk encryption for laptops or thumb drives)	PR.AA-06	PR.AA-06.02
FS SSG.072	**Cybersecurity awareness training:** All personnel receive cybersecurity awareness training upon hire and on a regular basis.	**3.J**	**Yes**	**Yes**	The organization should have a cybersecurity training program designed to increase employees' situational awareness of cybersecurity threats and knowledge of cybersecurity controls. As referenced, in PR.AT-01.02, training should support topics of situational awareness and competencies for data protection, personal data handling, compliance obligations, working with third parties, detecting cyber risks, and how to report any unusual activity or incidents. Organizations should maintain a record of all training received. Provide situational awareness training that is relevant to all personnel (full-time or part-time; permanent, temporary or contract) upon hire and on a regular basis. Prescribed training should be scoped and defined for areas where additional job-relevant requirements warrant additional validation. Provide information on any exceptions. As referenced in PR.AT-01.03, training should be updated on a regular basis to reflect the risks and threats identified by the organization, the organization's security policies and standards, applicable laws and regulations, and changes in individual responsibilities.	- Information and cybersecurity risk policy, standards, and procedures - Cybersecurity training standards, schedule, materials, and records (including metrics) - Job-relevant or job-specific cybersecurity training - Examples of cybersecurity training and situational awareness campaigns - Training records	PR.AT-01	PR.AT-01.01
FS SSG.073	**Cybersecurity awareness training content:** Cybersecurity awareness training includes, at a minimum, awareness of and competencies for data protection, personal data handling, compliance obligations, working with third parties, detecting cyber risks, and how to report any unusual activity or incidents.	**3.J**	**Yes**	**Yes**	The organization should have an organizational-wide information security training program designed to increase workforce situational awareness of information security threats and demonstrate minimum required knowledge of information security controls. The training program should consider the evolving and persistent threats and should include annual certification that personnel understand their responsibilities. Training can be provided by the organization or by a third-party training provider. Provide information as to what is included in the cybersecurity situational awareness training plan. Provide information that supports the training topics of situational awareness and competencies for data protection, personal data handling, compliance obligations, working with third parties, detecting cyber risks, and how to report any unusual activity or incidents.	- Information and cybersecurity risk policy, standards, procedure - Policy and procedure on reporting cyber incidents or unusual cyber activity - Cybersecurity training schedule, materials, and records, including timeframe training occurred (e.g., completion metrics) - Cybersecurity training materials and records (e.g., completion metrics) provided by third parties, if applicable - Third-party cybersecurity training policy, standards, and procedures - Examples of training	PR.AT-01	PR.AT-01.02

FS SSG.074	**Skill-specific training:** Mechanisms are in place to ensure that the personnel working with cybersecurity and technology (e.g., developers, DBAs, network admins, etc.) maintain current knowledge and skills related to changing threats, countermeasures, new tools, best practices, and their job responsibilities.	**3.J**	**Yes**	**Yes**	The organization's management should establish minimum standards and certifications for personnel and require continuing specialized education to ensure expertise is maintained. Training should be current and relevant. As threats change, training should be adopted to address the changing threat landscape. Personnel may maintain current knowledge through specific training programs, professional certifications, participation in industry groups, or other methods. Provide information on how the organization enables employees and their managers to identify courses that they feel would be of benefit to employees to aid in terms of increasing their skills or awareness, or keeping up to speed with the latest technologies, standards, processes, or threats. Describe which metrics, reporting, and gap analysis mechanisms are in place to ensure that the personnel working with cybersecurity and technology maintain currently knowledge and skills related to changing threats, countermeasures, new tools, best practices, and their job responsibilities. As referred to GV.RR-03.01, management should have a methodology in place to measure and document technology and cybersecurity risks to determine resources required for mitigating gaps.	- Cybersecurity training schedule, materials, and evidence of completion - Training-related description of services provided by training team - Certification requirements for cybersecurity personnel - Training and development plans - Review of training hours and effectiveness of training related to cybersecurity - Evidence of professional certifications, if applicable - Independent review of existing security capabilities and expertise - Examples of training	PR.AT-02	PR.AT-02.01
FS SSG.075	**Training of high-risk groups:** High-risk groups, such as those with elevated privileges or in sensitive business functions (including privileged users, senior executives, cybersecurity personnel and third-party stakeholders), receive cybersecurity situational awareness training for their roles and responsibilities.	**3.J**	**Yes**	**Yes**	Cybersecurity training should be aligned with the level of cybersecurity risk that exists within a business unit or high-risk group. The organization should develop a cybersecurity training program that includes learning goals and objectives that align cybersecurity with employee roles and responsibilities. Privileged users, such as network, systems, or database administrators, who are granted elevated access privileges and permissions, should have additional training that focuses on the management of system's security and the judicious use of their privileged access (e.g., insider threats). Users in sensitive business functions, who are granted elevated access privileges and permissions, should also receive cybersecurity additional awareness training for their roles, and the judicious use of their privileged access (e.g., Business Email Compromise). Describe how high-risk groups receive cybersecurity situational awareness training for their roles and responsibilities. Provide information on how situational awareness materials are made available to employees when prompted by highly visible cyber events or by regulatory alerts, and how workshops are held with senior management to provide them with situational awareness for vulnerability management and incident response.	- Cybersecurity training schedule and materials (including training provided to management) - Updated and maintained training-related description of services provided by training team - Examples of training	PR.AT-02	PR.AT-02.02
FS SSG.076	**Response and recovery plan training:** All personnel (employee and third party) are made aware of and are trained for their role and operational steps in response and recovery plans.	**4.B**	**Yes**	**Yes**	Roles and responsibilities must be clearly described in the incident response plan and communicated to all appropriate staff in order to maintain an organized and effective incident response process. The organization may use tabletop exercises or other testing to ensure personnel know their roles and responsibilities when an incident occurs. Describe how the organization's personnel know their roles and responsibilities and the operational steps when a response is needed. Describe the roles and responsibilities within the response process.	- 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	PR.AT-02	PR.AT-02.03

FS SSG.077	**Customer awareness training:** The organization has established and maintains a cybersecurity awareness program through which the organization's customers are kept aware of new threats and vulnerabilities, basic cybersecurity hygiene practices, and their role in cybersecurity, as appropriate.	--	--	**Yes**	The organization should inform and update customers of current cyber threats and ongoing cybersecurity risks. There are many ways to inform customers and stakeholders of cybersecurity risks including the organization's website (e.g., security requirements that customers should follow), email, or social media, etc. Provide information on how the organization has established and maintains a cybersecurity situational awareness program through which the organization's customers are kept aware of new threats and vulnerabilities, basic cybersecurity hygiene practices, and their role in cybersecurity, as appropriate. Describe how customer facing cybersecurity situational awareness materials are posted on the organization's public website.	- Samples of any documentation or website materials that support customer awareness communication programs - Samples of email and social media programs / documentation - Annual review of customer awareness training	PR.AT-02	PR.AT-02.06
FS SSG.078	**Data-at-rest protection:** Data-at-rest is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy (e.g., through the use of encryption, authentication, access control, segregation, masking, tokenization, and file integrity monitoring).	**3.K**	**Yes**	**Yes**	Data-at-rest is generally resident data stored on mobile devices, desktops, servers, within application and log files, databases, or storage repositories. Management is responsible for identifying where data resides, including data hosted by external service providers, and for determining whether encryption or other methods (e.g, sandboxing, authentication, access control, segregation, masking, tokenization, and file integrity monitoring) are necessary to protect data from unauthorized access or theft. Protection should ensure that data is unreadable at rest (e.g., through encryption). Encrypting passwords in storage and transmission can be achieved by various tools, methods or software specifically designed to protect the confidentiality of passwords. Encrypting data-in-transit communications containing passwords or transmitting cryptographic password hashes instead of plaintext passwords helps protect against threats to capture passwords. Provide information supporting how data-at-rest is protected based upon the criticality and sensitivity of the information in alignment with the data classification and protection policy. Describe the policies, standards, and controls in place for data at rest, including appropriate encryption, authentication, and access control, among others. When used, encryption algorithms must be recognized industry-wide and key management procedures must be in line with protection objectives.	- Data classification and protection policy - Physical and environmental information security policy - Managing electronic information security standard - Cryptography and key management standard - Password/PIN management security standard - Data-at-rest security documentation - Mobile device standards (laptop, removable media) - Evidence that data is encrypted - Data inventory	PR.DS-01	PR.DS-01.01
FS SSG.079	**Data loss prevention:** 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.	--	--	**Yes**	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.	- Data leakage prevention operations guide - Data leakage prevention monitoring - Security incident response policy, standard, plan, and process - Privileged access security standard - Device permissions standard - Related tool documentation - Network security standard - Behavioral analytic and rate limiting tools - Tool catalog	PR.DS-01	PR.DS-01.02

FS SSG.080	**Removable media protection:** The organization defines and implements controls for the protection and use of removable media (e.g., access/use restrictions, encryption, malware scanning, data loss prevention, etc.)	**3.R**	**Yes**	**Yes**	Removable media devices (USB, CD, and DVD) should be restricted for use, and monitored for inappropriate activity. For example, technology should be implemented to prevent users from attaching a USB drive to their portable or desktop system. Describe how the organization defines and implements controls for the protection and use of removable media and mobile devices. Describe the organization's access control procedures for approval on enabling access to removable media. Describe how removable media and mobile device use is restricted according to the organizations policies, procedures or controls for removable storage and restricted access. Provide information on the tools and processes utilized.	- Removable storage devices policy, standard, procedure - Mobile/communication devices policy, standard, and procedure - Related tools, examples, and reporting - Container controls/tools - Bring your own device (BYOD) user agreements - Evidence of endpoint protections preventing unauthorized use of removeable media and control standards enforcing appropriate use (e.g., encryption of removable media) - Evidence that antivirus and anti-malware tools are deployed on end-point devices (e.g., workstations, laptops, and mobile devices) and include configurations appropriate to removable media (scanning USB drives, CD/DVD upon connection, prevent boot to removable media) - Access control procedures for removable media	PR.DS-01	PR.DS-01.03
FS SSG.081	**Data-in-transit protection:** Data-in-transit is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy (e.g., through the use of encryption, authentication, access control, masking, tokenization, and alternate transit paths).	**3.K**	**Yes**	**Yes**	Data-in-transit includes two primary categories – data that is moving across public or "untrusted" networks such as the Internet, and data that is moving within the confines of private networks such as corporate Local Area Networks (LANs). Provide information on how data-in-transit is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy. Provide information in support of controls for data-in-transit including, but not restricted to, appropriate encryption, authentication, and access control. Provide information on other methods used to protect data-in-transit (e.g., masking, tokenization, alternate transit paths, etc.) Provide detail regarding the framework and controls as it pertains to data in transit. When used, encryption algorithms must be recognized industry-wide and key management procedures must be in line with protection objectives.	- 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-02	PR.DS-02.01
FS SSG.082	**Data-in-use protection:** Data-in-use is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy (e.g., through the use of encryption, authentication, access control, masking, tokenization, visual shielding, memory integrity monitoring, etc.)	**--**	**Yes**	**Yes**	Data-in-use is data that is actively being accessed and processed by a user. Authentication protections, least privilege access, and role-based access controls should be in place to combat unauthorized use and/or compromise. Describe safeguards (e.g., encryption, authentication, access control, masking, tokenization, visual shielding, memory integrity monitoring) implemented for data loss prevention. Provide information on how data-in-use is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy. Provide information on the related policies and standards. When used, encryption algorithms must be recognized industry-wide and key management procedures must be in line with protection objectives.	- Data-in-use security documentation - Evidence that data is encrypted - Data classification and protection policy - Physical access controls for network ports, collaborative computing devices, and applications - Access control policy and related procedures - Password/pin management standard - Access request process - Risk-based periodic access review	PR.DS-10	PR.DS-10.01

FS SSG.083	**Data backup and replication:** The organization defines and implements standards and procedures for configuring and performing backups and data replications, including defining backup requirements by data/application/infrastructure criticality, segregating (e.g., air-gapping) and securing backups, verifying backup integrity, and performing backup restoration testing.	**3.O**	**Yes**	**Yes**	A formal backup and recovery plan describes how critical systems are backed up and restored in the event of loss or corruption of production data. Backup and recovery methods and procedures must be consistent with defined data and system recovery time objectives, recovery point objective, and impact tolerance requirements. The organization's management should reassess backup and recovery strategies as the technology and threat environments evolve. Additionally, business units should evaluate the usability and integrity of the recovered data. Describe how the organization defines and implements standards and procedures for configuring and performing backups of information and data replications. Describe how the organization periodically conducts tests of backups to business assets (including full system recovery) to support cyber resilience. Describe any backup safeguard strategies and measures in place to mitigate ransomware attacks (e.g., air-gapping). Describe how the organization defines backup requirements by data/application/infrastructure criticality, segregating and securing backups, and verifying backup integrity. Provide information on how assets are classified and risk assessed in support of backup and testing strategy.	- Risk management frameworks and process documentation - Information classification - Data backup and recovery policy, standard, and process - Backup and restore standards and plans, inclusive of critical applications - Backup and restore testing standards and process - Formal backup and recovery testing documentation - Documentation evidencing annual tests of systems, applications, and data recovery - Data/system recovery time objectives, recovery point objectives, and impact tolerance requirements	PR.DS-11	PR.DS-11.01
FS SSG.084	**Configuration baselines:** The organization establishes and maintains standard system security configuration baselines, informed by industry standards and hardening guidelines, to facilitate the consistent application of security settings, configurations, and versions.	**3.M, 3.N, 3.P**	**Yes**	**Yes**	The organization should develop baseline security configuration standards for production systems based on risk and in accordance with applicable configuration guidelines. A baseline configuration represents an approved set of specifications for a system, or configuration item(s) within a system, such as enabled or disabled functions or security parameters (e.g., access or password characteristics). Provide information on how the organization establishes baseline system security configuration standards, factoring in vendor recommendations, industry standards, and hardening guidelines. Describe how the baseline security configuration standards facilitate consistent application of security settings to designated information assets. Describe how the organization determines the platforms (e.g., hardware, devices, software, operating systems, etc.) for which configuration standards will be developed. Describe the frequency and review and update of configuration standards for various platforms.	- Anti-virus and anti-malware control documentation - Monitoring dashboard reports comparing baselines against current configurations - Related security policies, standards, and procedures - Related configuration policies, standards, and procedures - Procedures relating to the use of centralized configuration management tools - List of baselines - Sample of baselines, including use/reference to industry standards or vendor recommendations	PR.PS-01	PR.PS-01.01
FS SSG.085	**Least functionality:** The organization's systems are configured to provide only essential capabilities to implement the principle of least functionality.	**3.M, 3.N, 3.S**	**Yes**	**Yes**	The principle of least functionality provides that information systems are configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, such as ports, protocols, and/or services that are not integral to the operation of that information system. The organization should securely configure network components operating systems, applications, databases, etc., to ensure that only approved ports, protocols, and services are allowed and disable all unnecessary services, ports, and protocols. Describe how the organization's systems are configured to provide only essential capabilities to implement the principle of least functionality. Document the security configuration standards for operating systems and components. Provide information on the process used.	- 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	PR.PS-01	PR.PS-01.02
FS SSG.086	**Configuration deviation:** The organization employs detection measures and performs regular enforcement checks to ensure that non-compliance with baseline security standards is promptly identified and rectified.	**3.N, 3.P**	**Yes**	**Yes**	Describe how the organization employs detection measures and performs regular enforcement checks to ensure that non-compliance with baseline system security standards are promptly identified and rectified, in accordance with their risk. Provide information on the detection measures, tools used and frequency of enforcement checks. Describe how criticality and risk is considered for remediation of identified risks.	- Software management security standard - Security baseline processes and procedures - Procedures for file integrity monitoring - Related tool and frequency documentation - Monitoring dashboard reports - Remediation management documentation - Routine rotation of devices with known clean images	PR.PS-01	PR.PS-01.03

FS SSG.087	**Encryption standards:** Acceptable encryption standards, methods, and management practices are established in accordance with defined industry standards.	**3.K**	**Yes**	**Yes**	The organization should establish encryption standards, methods, and management practices in accordance with defined industry standards. Responses should include evidence that the encryption standards, methods, and management practices are built upon these industry standards. Encryption algorithms must be recognized industry-wide and key management procedures must be in line with protection objectives. Provide information on the related standards, methods, and management practices.	- Encryption standards, methods, and management practices, including evidence of consistency with industry standards - Evidence of a process in place to modify the standards, methods, and/or practices due to changes in international, national, and financial services industry standards and guidelines	PR.PS-01	PR.PS-01.05
FS SSG.088	**Encryption management practices:** The organization employs defined encryption methods and management practices commensurate with the criticality of the information being protected and the inherent risk of the technical environment where used.	**3.K**	**Yes**	**Yes**	Data-at-rest, data-in-use, and data-in-transit should employ encryption methods and management practices to protect the confidentiality and integrity of data. Describe how the organization implements encryption methods and management practices commensurate with the criticality of the information being protected and the inherent risk of the technical environment where used. Responses should utilize a cryptography and key management standard or policy that is aligned to the cyber risk management program to identify inherent risk, and criticality of the information being protected to determine whether encryption is necessary to protect data from unauthorized access or theft. When used, encryption algorithms must be recognized industry wide and key management procedures must be in line with protection objectives.	- Cryptography and key management standard - Cryptographic algorithms standard - Encryption systems and key management documentation - Cyber risk management strategy and framework - Information classification policies, standards, procedures	PR.PS-01	PR.PS-01.06
FS SSG.089	**Cryptographic keys and certificates:** Cryptographic keys and certificates are tracked, managed, and protected throughout their lifecycles, to include for compromise and revocation.	**--**	**Yes**	**Yes**	Describe how the organization tracks, manages, and protects cryptographic keys and certificates throughout their lifecycle (e.g., from generation to destruction) while maintaining operational availability. Provide information of how an organization securely manages keys and certificates used for third party connections and within third party (e.g., Cloud) environments. For example, cryptography public and private keys that are distributed between sender and receiver should utilize a secure TLS or SSL connection to prevent compromise. Responses should provide information on established cryptography and key management standards implemented to ensure keys and certificates are securely managed to maintain confidentiality and integrity of an organization's sensitive information. Key revocation should be included within the cryptography key lifecycle to deactivate a public key certificate or symmetric encryption key that is compromised or no longer needed. Describe key revocation processes and procedures. Responses should include evidence of an organization enforcing cryptography standards and policies.	- Cryptography and key management standard - Cryptographic algorithms standard - Third party connection standards - Third party environment security standards (e.g., cloud environment standards)	PR.PS-01	PR.PS-01.07
FS SSG.090	**End-user device protection:** End-user mobile or personal computing devices accessing the organization's network employ mechanisms to protect network, application, and data integrity, such as "Mobile Device Management (MDM)" and "Mobile Application Management (MAM)" technologies, device fingerprinting, storage containerization and encryption, integrity scanning, automated patch application, remote wipe, and data leakage protections.	--	--	**Yes**	Organizations should establish and maintain an up-to-date inventory that is inclusive of external information systems (e.g., end-user mobile or personal computing devices). Processes should be in place to review inventories to ensure all devices accessing the organization's network are approved or removed if unauthorized. Provide information on how end-user mobile and/or personal computing devices accessing the organization's network employ mechanisms designed to protect network, application, and data integrity. Provide information on policies and procedures that are established for end-user mobile or personal computing devices designed to keep corporate data secure. Responses can provide evidence of "Mobile Device Management (MDM)" and "Mobile Application Management (MAM)" technologies, device fingerprinting, storage containerization and encryption, integrity scanning, automated patch application, remote wipe when a personal device is lost or stolen, and data leakage protections (e.g., end-user training).	- Inventory reports which depict external information systems, their key characteristics, and who manages them - Policies and procedures for maintaining inventory of external information systems - Diagrams or connectivity flow documentation - Evidence of mechanisms implemented to protect network, application, and data integrity - End user device protection software selection - End user device software configuration standards	PR.PS-01	PR.PS-01.08

FS SSG.091	**Patch identification and application:** The organization defines and implements controls to identify patches to technology assets, assess patch criticality and risk, test patches, and apply patches within risk/criticality-based target time frames.	**2.B, 3.S**	**Yes**	**Yes**	Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. Patch management is required by various security compliance frameworks, mandates, and other policies. For example, NIST Special Publication (SP) 800-532 requires the SI-2, Flaw Remediation security control, which includes installing security-relevant software and firmware patches, testing patches before installing them, and incorporating patches into the organization's configuration management processes. Similarly, ISO 27001 A.12.6.1, Management of Technical Vulnerabilities, requires the timely implementation of patches for newly discovered technical vulnerabilities to ensure the organization maintains acceptable risk levels. Another example PCI-DSS, which requires that the latest patches be installed and sets a maximum timeframe for installing the most critical patches. Effective patch management may include establishing procedures to stay abreast of patches, to test availability in a segregated environment, and to install them when appropriate. Describe the implemented controls used to identify patches to technology assets, assess patch criticality, and risk, and test and apply the patch within risk/criticality-based target time frames. Provide information on related tools and frequency.	- 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.)	PR.PS-02	PR.PS-02.01
FS SSG.092	**Asset maintenance:** The organization defines and implements controls for the on-site and remote maintenance and repair of the organization's technology assets (e.g., work must be performed by authorized personnel, use of approved procedures and tools, use of original or vendor-approved spare parts).	--	--	**Yes**	Describe the procedures, tools, and controls in place for the maintenance and repair of the organization's technology assets, including but not limited to off-premise assets such as cloud computing. Changes to assets should be formally documented within the change management process. Describe how physical entry controls, employee observation, equipment maintenance, removal of assets, and related controls are in place. Describe how the remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access or tampering. Describe the supporting processes and tools that are in place along with roles and responsibilities.	- Related policies, standards, and process (e.g., data center access, equipment maintenance, retiring of assets, and destruction of components) - Control environment around these processes - Monitoring dashboards - Inventory of assets - Asset maintenance logs or other metrics - Remote connectivity security standard - Privileged access security policy, standard, and process - Specific procedures related to vendor maintenance of assets - Related policies and procedures - Roles and responsibilities - Access request and review process	PR.PS-03	PR.PS-03.01
FS SSG.093	**Log management standards:** The organization establishes and regularly reviews log management standards and practices, to include the types of events to be detected, log content, security and access considerations, monitoring protocols, integrity checking mechanisms, and retention periods.	**3.Q**	**Yes**	**Yes**	A log record provides the ability to show who has accessed an information system, what operations the user has performed during a given period, errors preventing an application from running, and monitor users (both authorized and unauthorized) for access, authentication, usage, connections, devices, and anomalous behavior. Organizations should have a log management standards and practices that consider potential future needs for log use in forensic investigations and as forensic evidence. Describe how log management standards and practices have been established to include formal requirements for the types of events to be detected, explicit content to be logged, security and access considerations to prevent unauthorized access, monitoring protocols, integrity checking mechanisms, and retention periods. Provide information regarding the content and structure of logs. Describe how logs are reviewed and analyzed (e.g., input into the security operations center tool).	- Security event logging and monitoring policy, standard, and procedure - Evidence of log review for adequacy of log content, device reporting, and testing of alerting functionality	PR.PS-04	PR.PS-04.01

FS SSG.094	**Log coverage:** The organization defines the scope and coverage of audit/log records to be created and monitored (i.e., internal and external environments, devices, and applications/services/software to be monitored) and has controls in place to ensure that the intended scope is fully covered and that no logging failures are inhibiting the collection of required logs.	**3.Q**	**Yes**	**Yes**	Audit/log records are created to show traceability of who has accessed an information system, what operations the user has provided during a given period, errors preventing an application from running, and monitor users (both authorized and unauthorized) for access, authentication, usage, connections, devices, and anomalous behavior. Provide information on how logging and monitoring policies, standards, and procedures are established and managed to define the scope and coverage of audit/log records. Describe the coverage of internal and external environments, devices, and applications/software to be monitored. Describe how policies and/or controls are implemented to ensure that the intended scope is fully covered and that no logging failures are inhibiting the collection of required logs. Describe processes related to planning for logging failures (e.g., exceeding audit log storage capacity, access failures, hardware failure, etc.). Describe fail-safe logging mechanisms utilized when the primary logging capability fails related to alerting, alternate storage, shutdown of the system, etc.	- Security event logging and monitoring policy, standard, and procedure - Evidence of log review for adequacy of log content, device reporting, and testing of alerting functionality	PR.PS-04	PR.PS-04.02
FS SSG.095	**Log security and retention:** The organization's activity logs and other security event logs are generated, reviewed, securely stored, and retained in accordance with data retention obligations and established standards.	**3.Q**	**Yes**	**Yes**	All systems, including network devices should have logging enabled. The organization should maintain sufficient logs of physical and logical access to review an event. Information captured in logs is critical to detecting malicious activity and provide incident responders with crucial evidence for investigations. Logs may be modified by attackers, including insiders, to hide malicious activity. Logs should be reviewed periodically for completeness and to ensure they have not been deleted, modified, overwritten, or compromised. This is most easily accomplished by using a centralized server that maintains logs in a separate, secure location. Describe how the organization's activity logs and other security event logs are generated, reviewed, securely stored, and retained in a secure manner and in accordance with data retention obligations and established standards. Refer to PR.PS-04.01 and PR.PS-04.02, to establish log management standards and practices and define the scope and coverage of audit/log records to be created and monitored according to the data retention obligations and established standards. Provide information on the organization's review process of the audit/log records. Provide information on the storage and length of time event logs are stored in accordance with data retention policies, procedures, and standards.	- Security event logging and monitoring policy, standard, and procedure - Data retention policy, procedure, and standard - Examples of tools used - Related procedure documents - Evidence of logs and configuration settings matching log retention documentation - Evidence of segregation of access between logging sources and storage location	PR.PS-04	PR.PS-04.03
FS SSG.096	**Malware prevention:** The organization has policies, procedures, and tools in place to detect and block malware from infecting networks and systems, including automatically updating malware signatures and behavior profiles on all endpoints.	**3.M, 4.A**	**Yes**	**Yes**	Malware has become more and more sophisticated in recent years, evolving from annoyance attacks or proof-of-concept attacks to rootkits and key loggers designed to steal critical business data. Anti-virus and anti-malware tools help protect data and systems by detecting malicious code or malware, such as viruses, Trojans, rootkits, and destructive malware. Having antivirus and malware protection on systems, desktops, laptops, and other devices is critical given today's threats. The organization should implement and actively manage anti-virus and anti-malware software, including regular updates based on the risk profile of the organization. Describe the policies, procedures, and tools in place to detect and block malware from infecting networks and systems. Describe how the organization has processes to automatically update malware signatures and behavior profiles on all endpoints. Provide information on malware protection and intrusion protection. Describe process to identify devices that have not been updated within a given period of time (i.e., inaccessible).	- Anti-malware security standards and procedures - Proof that anti-virus and anti-malware tools are deployed on end-point devices (e.g., workstations, laptops, and mobile devices) and used to detect attacks - Forensic security standards and procedures - Proof that mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks - Proof that up-to-date antivirus and anti-malware tools are used - Related reporting to management - Proof that programs that can override system, object, network, virtual machine, and application controls are restricted	PR.PS-05	PR.PS-05.01

FS SSG.097	**Mobile code prevention:** The organization implements safeguards against unauthorized mobile code (e.g., JavaScript, ActiveX, VBScript, PowerShell, etc.) on mobile, end point, and server systems.	**3.M, 4.A**	**Yes**	**Yes**	Mobile code is any program, application, or content that can be transmitted across a network and run-on a variety of platforms (e.g., JavaScript, ActiveX, VBScript, PowerShell, etc.). Mobile code usage should be limited and restricted to defined authorized uses on mobile, end point (e.g., laptops, workstations), and server systems. Policies and procedures should be in place to outline the acceptable and unacceptable uses of mobile code in systems to prevent from malware. Provide information on how the organization monitors the use of mobile code (e.g., audit logs) to detect unauthorized use. Describe safeguards implemented (e.g., network intrusion detection systems, intrusion prevention systems to monitor network traffic) on mobile, end point, and server systems to combat unauthorized mobile code.	- Removable storage device policies, standards, and procedures - Mobile device security policies, standards, and procedures - Managing electronic information policies, standards, and procedures - Storage security policies, standards, and procedures - Related patch deployment policies, standards, and procedures - BYOD policies, standards, and procedures - Proof that anti-virus and anti-malware controls are in place to detect attacks and alert management.	PR.PS-05	PR.PS-05.02
FS SSG.098	**Email and message service protection:** The organization has policies, procedures, and tools in place to detect, isolate, and block the use of attached malware or malicious links present in email or message services.	**3.L, 4.A**	**Yes**	**Yes**	The three major protocols used for the majority of electronic mail (POP, IMAP and SMTP) are clear text protocols that were designed without security or privacy in mind. An organization's email can be subject to interception, alteration and counterfeiting by anyone on the virtual path between the sender and the recipient. Spear phishing and whale phishing are common social engineering attacks that use fraudulent emails to acquire sensitive information or financial gain. As referenced in PR.AT-01.01, organizations should have cyber awareness trainings in place that educate personnel on secure email use, phishing attempts, and malicious links present in email or message services. As such, the organization should implement email or message services protection mechanisms to protect the organization from malware or viruses. Describe which policies, procedures, and tools are in place to automatically scan, detect, isolate, and block the use of attached malware or malicious links presented in email or message services. Provide information on the tools utilized.	- Information classification policies, standards, procedures - Managing electronic information policies, standards, procedures - Email server security standards - Proof that email protection mechanisms are used to filter for common cyber threats (e.g., attached malware or malicious links) - Messaging system security standards - Anti-malware security standards - Other related policies, standards, and procedures - Anti-virus and anti-malware controls - Proof that antivirus and anti-malware tools are used to detect attacks - Training examples and attestation - Tool examples - Related reporting - Procedures for updating malware signatures and behavior patterns	PR.PS-05	PR.PS-05.03
FS SSG.099	**Secure SDLC processes:** The organization implements Secure Systems Development Lifecycle processes for in-house software design, configuration, and development, employing best practices from secure-by-design methodologies (e.g., secure coding, code review, application security testing, etc.) during all phases of both traditional and agile projects.	**--**	**Yes**	**Yes**	The secure System Development Life Cycle (SDLC) is the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal. For any SDLC, information security should be integrated to ensure appropriate protection of the information that the system will transmit, process, and store. Security should be integrated during all phases of both traditional and agile projects. Secure-by-design methodologies (e.g., secure coding, code review, application security testing, etc.) should apply to both traditional and agile projects during all phases. Describe the process for secure system development, including supporting infrastructure and any "off-the-shelf" applications. Provide information supporting secure SDLC for in-house software design, configuration, and development. Describe how the organization employs best practices from secure-by-design methodologies and vendor recommendation during all phases of both traditional and agile projects.	- Application security processes and procedures including testing for common vulnerabilities (OWASP), code integrity - System development lifecycle documentation - Related development documentation - Developer training documentation - Source code analysis processes and procedures - DevSecOps processes and procedures - Platform environment specific development standards and practices	PR.PS-06	PR.PS-06.01

FS SSG.100	**Target environment security design:** The architecture, design, coding, testing, and operationalization of system solutions address the unique security, resilience, technical, and operational characteristics of the target platform environment(s) (e.g., distributed system, mainframe, cloud, API, mobile, database, etc.)	--	**Yes**	**Yes**	As mentioned in PR.PS-06.01, the secure System Development Life Cycle (SDLC) is the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal. Provide information supporting the SDLC process addressing the unique security, resilience, technical, and operational characteristics of the target platform environment(s). Describe how software development integrates robust resilience (e.g., threat modeling, secure design principles, etc.). Testing of system solutions should be performed to validate the functionality, performance, and alignment of resilience, technical, and operating characteristics of the target platform environment(s). Different target implementation platforms and environments (e.g., distributed systems, mainframe, cloud, API, mobile, database, etc.) will have unique security best practice characteristics. Describe the secure SDLC practices that may be specific to development for each target platform or environment (e.g., based on vendor recommendations).	- Secure system development standards and processes, including how cybersecurity risk is incorporated during the beginning of processes - Security testing standards, processes, and reports - Other related policies, standards, and procedures - Platform/environment specific secure SDLP standards& practices - DevSecOps practices and procedures	PR.PS-06	PR.PS-06.02
FS SSG.101	**System requirements management:** Functional, operational, resilience, and security requirements for system development and implementation projects are documented, agreed to by relevant stakeholders, and tracked and managed through development, testing, assurance, acceptance, and delivery.	--	**Yes**	**Yes**	Functional, operational, resilience, and security requirements should be established and managed within the SDLC process. Provide information to support that functional, operational, resilience, and security requirements are agreed upon by relevant stakeholders. Describe how each phase of the SDLC process (e.g., development, testing, assurance, acceptance, and delivery) is tracked and managed. Describe the use of requirements traceability matrices, burn-down charts, or other tools to track and manage stakeholder requirements in the SDLC process.	- Secure system development standards and processes - System development lifecycle documentation - Evidence of fundamental, operational, resilience, and security requirements - Related SDLC tracking/management documentation - Stakeholder approvals and/or SDLC meeting minutes - Requirements traceability matrices	PR.PS-06	PR.PS-06.03
FS SSG.102	**Development and testing security:** Systems development and testing tools, processes, and environments employ security mechanisms to protect and improve the integrity and confidentiality of both the SDLC process and the resulting product (e.g., secured code repositories, segmented environments, automated builds, etc.)	--	**Yes**	**Yes**	System development and testing tools, processes, and environments should incorporate security mechanisms to protect and improve the integrity and confidentiality of both the SDLC process and the resulting product. The organization should implement security measures to protect the systems and data used during the development lifecycle. Organizations should have a separation between production and non-production environments, control identity and access management, identify vulnerabilities to be remediated, and protect data against unauthorized access. Further, the organization should follow development practices (e.g., DevSecOps) and tactics (e.g., CI/CD) to improve the SDLC processes, security, and confidentiality.	- Application security processes and procedures including testing for common vulnerabilities (OWASP), code integrity - System development lifecycle documentation - Evidence of implemented security mechanisms for system development and testing tools, processes, and environments	PR.PS-06	PR.PS-06.04
FS SSG.103	**Testing and validation strategy:** A software security testing and validation strategy is developed and implemented in the development lifecycle of all software projects, defining testing requirements and plans; performing/automating testing, vulnerability scanning, and migration activities; and supporting code integrity verification (e.g., using digital signatures).	--	**Yes**	**Yes**	Newly created software may have security weaknesses; therefore, the organization should assess the cyber risks before applications are released for business use. Provide information on how the organization defines testing requirements and plans. Describe how the organization assesses the cyber risks of software prior to deployment using penetration testing and/or vulnerability scanning. Provide information on the assessment process and any tools used. Provide information on how the security testing and validation strategy is implemented throughout the development lifecycle of all software projects. Describe how the organization develops and implements a software security testing and validation strategy. Responses should include code integrity verifications implemented in the development lifecycle for all software projects. Describe how security testing tools and procedures are adapted to the various platforms and environments in use (e.g., mainframe, mobile, etc.).	- Security testing standard for applications - Related testing documentation - Migration activities - Application security processes and procedures including testing for common vulnerabilities (OWASP), independent code review and code integrity - System development lifecycle documentation - Related development documentation - Developer training documentation - Source code analysis processes and procedures - Platform/environment specific testing tools and procedures	PR.PS-06	PR.PS-06.05

FS SSG.104	**Vulnerability remediation:** The system development lifecycle remediates known critical vulnerabilities, and critical vulnerabilities discovered during testing, prior to production deployment.	--	**Yes**	**Yes**	Describe how the organization has established and maintains capabilities for ongoing vulnerability management, including systematic scans as part of SDLC policies, standards, and processes. Provide information on SDLC development and deployment practices (e.g., DevSecOps) and tactics (e.g., CI/CD pipelines) that can help identify and remediate critical vulnerabilities prior to production deployment. Responses include automated security testing capabilities to identify vulnerabilities early in the software development process. Describe how the organization performs testing to identify vulnerabilities prior to deployment. Provide information on the assessment process and any tools used. Describe how any exceptions are documented, assessed, and approved.	- Security testing standard for applications - Related testing documentation - Application security processes and procedures including testing for common vulnerabilities (OWASP), independent code review and code integrity - System development lifecycle documentation - Related development documentation - Developer training documentation - Source code analysis processes and procedures - Vulnerability exception management process	PR.PS-06	PR.PS-06.06
FS SSG.105	**Development and operational process alignment:** DevOps/DevSecOps practices and procedures are aligned with Systems Development Lifecycle, security operations, and technology service management processes.	--	--	**Yes**	The organization should adopt DevOps/DevSecOps practices and procedures, as appropriate, to ensure there is security testing incorporated during every phase of the SDLC. The organization should integrate security practices throughout the SDLC to reduce, mitigate and remediate the number of vulnerabilities prior to production deployment, and shorten the timeframe of the development lifecycle. Responses include alignment of practices, procedures, and processes for a more secure, robust Systems Development Lifecycle. Describe how DevOps/DevSecOps practices and procedures are aligned with Systems Development Lifecycle, security operations, and technology service management processes.	- DevOps/DevSecOps practices and procedures - Security testing standard for applications - Related testing documentation - Application security processes and procedures including testing for common vulnerabilities (OWASP), independent code review and code integrity - System development lifecycle documentation - Related development documentation - Developer training documentation - Source code analysis processes and procedures	PR.PS-06	PR.PS-06.07
FS SSG.106	**Database and data platform security:** The organization establishes policies and procedures for the secure design, configuration, modification, and operation of databases, data stores, and data analytics platforms consistent with the criticality of the data being managed.	--	--	**Yes**	The organization should establish policies and procedures for the effective implementation and secure design, configuration, modification, and operation of databases, data stores, and data analytics platforms. Policies and procedures should also specifically address privileged user and automated system connections (i.e., service connections) to databases and data stores. Policies and procedures should reflect considerations of the criticality of the data being managed and potential to adversely impact the organizational operations. Provide information of established configuration management policies and procedures.	- Related security policies, standards, and procedures - Related configuration policies, standards, and procedures	PR.PS-06	PR.PS-06.10
FS SSG.107	**Network segmentation:** Networks, systems, and external connections are segmented (e.g., using firewalls, software-defined networks, guest wireless networks, etc.) to implement defense-in-depth and access isolation principles.	**3.I, 3.S**	**Yes**	**Yes**	The organization should ensure networks, systems, and external connections are segmented (e.g., implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks). Segmenting is evidenced by using separate local area networks, virtual local area networks, or similar controls which can restrict or monitor network access as appropriate for the organization's risk. For example, networks with critical infrastructure should be segmented such that shell or administrative access is not available from the general desktop networks and only available via hardened jump servers. Provide information on how the organization's networks, systems, and external connections are segmented to implement defense-in-depth and access isolation principles.	- Network perimeter security policy, standard, and procedures describing separate trust/security zones - Internal corporate network security policy, standard, and procedures describing separate trust/security zones - Network management policy, standard, and procedures - Mobile device security standard - Related framework and strategy documents - Network security diagrams, security architecture, etc.	PR.IR-01	PR.IR-01.01
FS SSG.108	**Network device configurations:** Network device configurations (e.g., firewall rules, ports, and protocols) are documented, reviewed and updated regularly and upon change to ensure alignment with network access, segmentation, traversal, and deny-all default requirements.	**3.I, 3.S**	**Yes**	**Yes**	Network device configurations (e.g., firewall rules, ports, and protocols) should be aligned to defined security baseline configurations. A methodology should be implemented to determine if the organization is failing to meet, is meeting, or is exceeding those established benchmarks. Provide information on how network configurations are documented, formally reviewed, and agreed-upon. Describe how network device configurations are updated regularly and upon change to ensure alignment with network access, segmentation, traversal, and deny-all default requirements.	- Network device baseline configuration documents - Monitoring dashboard reports comparing baselines against current configurations - Related network device configuration policies, standards, and procedures - Procedures relating to the use of centralized configuration management tools	PR.IR-01	PR.IR-01.02

FS SSG.109	**Network communications integrity and availability:** The integrity and resilience of the organization's communications and control network services are enhanced through controls such as denial of service protections, secure name/address resolution, and/or alternate communications paths.	--	--	**Yes**	An organization's network perimeter enables or restricts connection to, and communication with, the internet. To control network traffic, the organization should use devices such as border routers and firewalls to restrict and filter traffic. These tools should be securely configured and maintained with current operating systems. Protection controls such as network segmentation, firewalls, and physical access controls to network equipment can be utilized to strengthen the integrity and resilience of an organization. Network architecture and network services design gives specific consideration to resilience, integrity, and security factors. Design principles such as zero trust architecture can be used as an alternative to enhance the control network services. Describe controls established (e.g., denial of service protections, secure name/address resolution, and/or alternate communications paths) to enhance the organization's communications and control network services.	- Internal network security standard - Network management standards - Network perimeter security standard - Other related policies, standards, and procedures - Risk assessments - Tools and controls examples - Data flow diagrams - Network diagrams showing firewall or other boundary protection devices segmenting DMZ and internal security zones - Zero trust architecture, if applicable - Evidence of lifecycle and configuration management for boundary protection devices - Network architecture	PR.IR-01	PR.IR-01.03
FS SSG.110	**Wireless network protection:** 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).	--	**Yes**	**Yes**	Wireless networks should include end-to-end encryption and strong authentication protocols (e.g., WPA2 + AES). Appropriate controls should exist on any wireless network to prevent unauthorized traffic from entering the network by appropriately segregating wireless and guest wireless networks. Provide information as to how the organization controls access to its wireless networks and the information that these networks process. Describe the mechanisms and tools utilized (e.g., appropriate authentication protocols).	- Network perimeter security policy, standard, and procedures - Internal corporate network security policy, standard, and procedures - Network management policy, standard, and procedures - Mobile device security standard - Related framework and strategy documents - Network device baseline configuration documents - Network architecture	PR.IR-01	PR.IR-01.04
FS SSG.111	**Remote access protection:** Remote access is carefully controlled (e.g., restricted to defined systems, access is actively managed (e.g., session timeouts, logging, forced disconnect, etc.), and encrypted connections with multi-factor authentication are used).	**3.F**	**Yes**	**Yes**	Remote access enables network troubleshooting, updates, and maintenance. Security controls (e.g., encryption, access roles and privileges, strong authentication, patching, access logging, auditing) should be in place to effectively protect against the numerous risks that remote access poses to the organization. Controlled and restricted remote access should include network and system administrators. Remote access should have encrypted connections with multi-factor authentication. Describe how the organization implements multi-factor authentication or equally secure access controls for remote access. Describe how remote access is carefully controlled and restricted to necessary systems. Necessary systems may include components, applications and/or devices. Describe how all types of external connections into the corporate network (e.g., employees, third-parties, virtual, desktops, etc.) are carefully controlled and restricted to necessary systems.	- Computer system access control policy - Network security standard - Remote connectivity security policy, standard, and procedures - Authentication security policy, standard, and procedures - Secure remote working awareness materials - Documented rationales for the risk-based decisions regarding the use or non-use of MFA - Various system security documentation - User access review (VPN, PIN logon, etc.) - Remote access and/or telecommuting security policy and procedures	PR.IR-01	PR.IR-01.05
FS SSG.112	**Production environment segregation:** The organization's production and non-production environments and data are segregated and managed to prevent unauthorized access or changes to the information assets.	--	**Yes**	**Yes**	Separation of non-production (e.g., development) from the production environment is important to safeguarding the confidentiality and integrity of information. Production data must be maintained with the same level of control if used for acceptance testing. All environments must maintain strong security controls, and movement of code or data between environments should be protected. Provide information on how the organization's production is separate from the non-production environment (logically/physically). Provide information on the network segmentation. Describe how data (both non-production and production) is protected, managed, and not used in inappropriate environments to prevent unauthorized access or changes to the information assets. Describe the access controls established to ensure that developers, administrators, and other privileged users reduce the exposure to production data. In particular, the organization's controls in place for backdoor production data changes and corrections that need to be made and documented.	- Database security standard - Network details and diagrams - Network security standards - Server inventory and standards - Web technologies security standard - Software development lifecycle documentation - Developer and administrator access controls - Production data change management procedures	PR.IR-01	PR.IR-01.06

FS SSG.113	**Operational and IoT technologies:** The organization defines and implements controls for securely configuring and operating Operational Technologies, Industrial Control Systems, and Internet-of-Things (IoT) devices (e.g., segregated printer networks, resetting of default passwords, etc.)	**3.I**	**Yes**	**Yes**	The organization should define, implement, and actively manage controls for securely configuring and operating Operational Technologies, Industrial Control Systems, and Internet-of-Things (IoT) devices. Organizations should maintain an inventory of Operational Technologies, Industrial Control Systems, and Internet-of-Things (IoT) devices. In financial institution environments, operational technologies generally include services such as printers, faxes, ATM's, cash management devices, security systems, video surveillance systems, and audio/video conference systems. Baseline configuration should be defined and established for Industrial Control Systems and network of connected devices to maintain security principles throughout configuration. Organizations should use a segmented network for Operational Technologies, as appropriate. Effective policies, procedures, and security controls should be implemented to mitigate risk and potential vulnerabilities. Describe security standards in place for operating all types of assets including Operational Technologies, Industrial Control Systems, and Internet-of-Things (IoT) devices. Describe how controls are defined and implemented for securely configuring and operating devices (e.g., physical access controls, least functionality). Describe standards, and controls in place for physical access security of operating Operational Technologies, Industrial Control Systems, and Internet-of-Things (IoT) devices.	- Network device baseline configuration documents - Controls implemented for secure configurations - Related network device configuration policies, standards, and procedures - Procedures relating to the use of centralized configuration management tools - Inventory of operational technology systems	PR.IR-01	PR.IR-01.07
FS SSG.114	**End-user device access:** The organization implements policies, procedures, end-user agreements, and technical controls to address the risks of end-user mobile or personal computing devices accessing the organization's network and resources.	--	**Yes**	**Yes**	Provide information on established policies, procedures, and end-user agreements for defining and permitting use of acceptable technology, social media, and personal devices for all personnel (employees and third party). Describe how the acceptable use policies, procedures, and agreements permit access to the organization's information systems and networks. Inappropriate use exposes the organization to potential risks (e.g., unauthorized access, compromise of network systems). Describe technical controls (e.g., VPN, antivirus software, password requirements) implemented to address the risks of end-user mobile and/or personal computing devices accessing the organization's network and resources. Describe how the organization implements mechanisms to restrict access to websites or services that do not serve legitimate business needs or purposes. Provide information on approval and authorization processes for all personnel to access the organization's applications and network through personnel devices. Describe the process of all personnel reviewing and accepting acceptable use policies.	- Related policies and procedures - End-user agreements - BYOD policies - Related employee training - Data encryption - Technical controls to address risks of personal devices accessing the organization's network and resources	PR.IR-01	PR.IR-01.08
FS SSG.115	**Physical and environmental controls:** The organization designs, documents, implements, tests, and maintains environmental and physical controls to meet defined business resilience requirements (e.g., environmental monitoring, dual power and communication sources, regionally separated backup processing facilities, etc.)	--	--	**Yes**	Environmental and physical controls (e.g., temperature and humidity controls or water damage protection for data centers or server rooms) ensure the availability of the organization's systems. Physical access controls for data centers should have surveillance controls at entry points, exit points, and inside, as well as geographical location controls to ensure faster latency, and recovery. The organization's environmental and physical controls should be designed according to resilience strategies and framework, and technology architecture in place. Physical controls should control and restrict entry and exit to organization's areas including, entry points in barriers, keycard-controlled doors, screening measures at entry points, and training for personnel who work in sensitive areas, etc. Environment controls should help organization's operate at a reasonably well-controlled environment, including fire suppression and detection devices, automatic emergency lighting during power outages, etc. Describe how environmental and physical controls are designed, documented, implemented, tested, and maintained to meet defined business resilience requirements. Provide testing performed on environmental and physical controls to ensure effectiveness.	- Documentation of environmental and physical controls - Business continuity/resiliency plans - Data backup and recovery policy, standard, and process - Backup and restore standards and plans, inclusive of critical applications - Backup and restore testing standards and process - Formal backup and recovery testing documentation - Documentation evidencing annual tests of systems, applications, and data recovery - Resilience strategy and framework - Technology Architecture	PR.IR-02	PR.IR-02.01

FS SSG.116	**Alternative resilience mechanisms:** The organization implements mechanisms (e.g., failsafe, load balancing, hot swaps, redundant equipment, alternate services, backup facilities, etc.) to achieve resilience requirements in normal and adverse situations.	--	--	**Yes**	Describe how the organization implements mechanisms (e.g., failsafe, load balancing, hot swap, redundant equipment, alternate sites, backup facilities, etc.) to achieve resilience requirements in normal and adverse situations. Mechanisms should be established to ensure the organization can resume critical business services after disruption. For example, backup facilities can be used for resumption of services when critical services are disrupted, or data is rendered corrupted, or inaccessible. The organization's mechanisms should be designed according to resilience strategies, and technology architecture in place. Provide information on risk assessment and tier strategy where applicable. Provide implementation strategy information related to normal vs. adverse situations.	- Data center recovery strategy and procedures - Asset risk assessment criteria and evaluation process - Business continuity, resiliency, incident management, and disaster recovery plans - Third-party policies, standards, and procedures - Evidence that critical online systems and processes are tested to withstand stresses for extended periods (e.g., DDoS) - Evidence of testing the ability to shift business processes or functions between different processing centers or technology systems for cyber incidents without interruption to business or loss of productivity or data - Resilience strategy - Technology architecture	PR.IR-03	PR.IR-03.01
FS SSG.117	**Utilization monitoring:** Baseline measures of network and system utilization and transaction activity are captured to support capacity planning and anomalous activity detection.	--	--	**Yes**	Organizations should maintain baseline measures of network, system utilization and transaction activity that are captured to support capacity planning and anomalous activity detection. The organization should identify hardware, software, and network components, internal and external connections, and types of information passed between systems to facilitate the development of a defense-in-depth security architecture and ensure appropriate network security. Network diagrams should be comprehensive, up-to-date and include inventoried assets. Processes and procedures should describe how the organization identifies, establishes, documents, and manages a baseline measure of network, system utilization, and transaction activity. Provide information supporting mapping of resources, connections, and data flows. Describe the organization's use of operational and network monitoring tools in the environment. Describe how operational and network monitoring intersect with event detection, incident identification, and incident management processes.	- Inventory of network resources and network connections - Related baseline measures - Related network diagrams and reporting showing connectivity and data flows - Related assessments - Related processes and procedures - Verification that network and system diagrams are stored in a secure manner with proper restrictions on access - Validation of an accurate asset inventory - Incident management procedures - Capacity planning analyses and estimates	PR.IR-04	PR.IR-04.01
FS SSG.118	**Availability and capacity management:** Technology availability and capacity is planned, monitored, managed, and optimized to meet business resilience objectives and reasonably anticipated infrastructure demands.	--	--	**Yes**	Provide information on how the organization maintains appropriate technology availability and capacity. Describe how the organization plans, monitors, manages, and optimizes technology availability and capacity to meet resilience objectives and reasonably anticipated infrastructure demands. Describe the linkage to availability requirements and risk assessment. Describe service level management and baselines including any scheduled downtime.	- Capacity management policy - Service level management standard - Service review process documentation - Inventory system - Operations reporting - Related risk and control assessments	PR.IR-04	PR.IR-04.02
	DETECT							
FS SSG.119	**Intrusion detection and prevention:** The organization deploys intrusion detection and intrusion prevention capabilities to detect and prevent a potential network intrusion in its early stages for timely containment and recovery.	--	**Yes**	**Yes**	Intrusion detection or prevention systems, anti-virus software, and endpoint detection can be used to help identify unusual activity by analyzing network traffic or code and alerting or taking action (e.g., blocking traffic that enters the network). Intrusion detection or prevention systems may include detecting potential insider threat activity. For example, incidents that may relate to insider threat may include failed log-in attempts, transfers of large amounts of data, altered coding on sensitive files, or personnel issues. Describe both host and network-based intrusion detection and prevention capabilities deployed to detect and prevent a potential network intrusion in its early stages for timely response, containment, and recovery. Provide information regarding the layers of protection.	- Intrusion detection policy and procedures - Insider threat policy and procedures - Intrusion detection alert metrics (e.g., number of alerts, types of alerts, monthly or quarterly reports,) - Process description - Proof of analyzing potential unusual activity - Proof that mechanisms or tools are in place to alert management to potential attacks (e.g., antivirus alerts, log event alerts) and trigger the incident response plan - Proof of related reporting	DE.CM-01	DE.CM-01.01

FS SSG.120	**Network traffic volume monitoring:** The organization implements mechanisms, such as alerting and filtering of sudden high volumes and suspicious incoming traffic, to detect and mitigate Denial of Service, "bot", and credential stuffing attacks.	--	--	**Yes**	Identification of disruptive cyber-attacks such as Denial of Service (DoS)/Distributed Denial of Service (DDoS) attacks relies on a coordinated collection and analysis of performance data and alerts, often including third-party providers such as upstream internet service providers (ISPs). Many risk-based tools are available to monitor uptime and system responsiveness. The organization should devise and implement mitigation approaches according to the organization's risk exposure. Describe the mechanisms implemented to detect and mitigate Denial of Service, "bot", and credential stuffing attacks. Provide information on alerting and filtering procedures when experiencing a sudden high volume of suspicious incoming traffic.	- Monitoring/detection policies and procedures - Process description - Proof of monitoring of potential attacks - Proof that mechanisms and tools are in place to alert management to potential attacks (e.g., antivirus alerts, log event alerts) - Proof that a risk-based solution is in place at the institution or Internet hosting provider to mitigate disruptive cyber-attacks (e.g., DoS/DDoS attacks) - Proof of related reporting	DE.CM-01	DE.CM-01.02
FS SSG.121	**Unauthorized network connections and data transfers:** The organization has policies, procedures, and tools in place to monitor for, detect, and block unauthorized network connections and data transfers.	--	--	**Yes**	The organization should have a comprehensive system for monitoring unauthorized access to systems, devices, components, and software. For example, automated processes or tools can detect and prevent changes to hardware or software and can alert management when certain attempted changes are executed. Describe the tools used to monitor, detect, and block access from/to devices, network connections, data transfers and API activity. Provide information on the approved policies and procedures. Provide information on how the various tools achieve the security objectives.	- Network security policies, standards, and procedures - Remote connectivity security policies, standards, and procedures - Business systems security policies, standards, and procedures based on applications that provide integrated data, video, and voice in one supported product - Network management policies, standards, and procedures - Internet connection policies, standards, and procedures - Allow or deny lists - Proof that mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks - Proof that processes are in place to monitor for the presence of unauthorized users, devices, connections, and software - Documents on related tools for preventing, monitoring, and remediating unauthorized access from/to devices, connections and data transfers are in place - Proof that role-based access reviews are effective and timely - Related reporting	DE.CM-01	DE.CM-01.03
FS SSG.122	**Unauthorized device connection:** The organization has policies, procedures, and tools in place to monitor for, detect, and block access from/to devices that are not authorized or do not conform to security policy (e.g., unpatched systems).	**3.R**	**Yes**	**Yes**	The organization should have a system for monitoring devices and connections that are not authorized or do not conform to security policy. For example, vulnerability scanning tools can monitor and detect unpatched systems, deny connection, and alert management. Organizations may employ device fingerprinting, certificates, or other methods to identify authorized devices. Describe the tools used to monitor, detect, and block access from/to devices and connections. Provide information on the approved policies and procedures. Provide information on how the various tools achieve the requirement.	- Related tools - Related reporting - Applications and supporting infrastructure security testing policies, standards, and procedures - Vulnerability management security policies, standards, and procedures - Proof that vulnerability scans are utilized to provide insight into the effectiveness of the patch management process	DE.CM-01	DE.CM-01.04
FS SSG.123	**Website and service blocking:** The organization implements measures to detect and block access to unauthorized, inappropriate, or malicious websites and services (e.g. social media, messaging, file sharing).	--	**Yes**	**Yes**	Describe the measures (e.g., web-filtering tools) implemented to detect and block access to unauthorized, inappropriate, or malicious websites and services. Provide information on tools used. Describe the organization's policy for connections to file sharing sites (e.g., DropBox, Box, etc.), and any procedures allowed to request exceptions. Describe how users can request exceptions to site blocking when required for business purposes.	- 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-01	DE.CM-01.05

FS SSG.124	**Anomalous activity detection:** The organization's controls include monitoring and detection of anomalous activities and potential intrusion events across the organization's physical environment and infrastructure, including the detection of environmental threats (fire, water, service outages, etc.) and unauthorized physical access to high-risk system components and locations.	--	**Yes**	**Yes**	Organizations should utilize monitoring and detection mechanisms and tools for the physical environment (e.g., entrances, restricted areas, confidential data repositories, vault areas, ATMs, etc.) and infrastructure, including any cloud infrastructure, if applicable. Describe how the organization's controls include monitoring and detection of anomalous activities and potential intrusion events across the organization's physical environment and infrastructure. Provide information on controls that detect environmental threats. Provide information on controls that detect unauthorized physical access to high-risk system components and locations (e.g., data centers, LAN closets, network cabling, etc.).	- 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-02	DE.CM-02.01
FS SSG.125	**Personnel activity monitoring:** 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.	**3.E**	**Yes**	**Yes**	The organization should have a comprehensive system for monitoring access to critical and mission critical systems, devices, components, software, and data for unauthorized access. Describe what controls are in place to actively monitor users (both authorized and unauthorized) for access, authentication, usage, connections, devices, and anomalous behavior to rapidly detect potential cybersecurity events. Describe any tools employed to monitor user activity within the environment. Describe the organization's monitoring controls interaction with the insider threat program.	- Event logging and monitoring policy, standard, and process - Description of controls - Use cases - Proof of related reporting - Proof that mechanisms and tools are in place to alert management of potential misuse (e.g., antivirus alerts, log event alerts) - Proof that roll-based monitoring of access to critical systems by third parties for unauthorized or unusual activity occurs - Proof of monitoring users with elevated privileges - Proof that processes are in place to monitor for the presence of unauthorized users, devices, connections, and software - Insider threat program	DE.CM-03	DE.CM-03.02
FS SSG.126	**Privileged account monitoring:** The organization logs and reviews the activities of privileged users and accounts, and monitoring for anomalous behaviors is implemented.	--	--	**Yes**	The organization should identify and perform logging of key systems, applications and devices and review logs on a regular basis, based on the risk profile of the organization. The organization should maintain a list of privileged users, and review and update the list of privileged users on a regular basis in accordance with the organization's policies and procedures. Describe how the organization performs logging and monitoring. Provide information regarding the review of system activities of privileged users and accounts, and how monitoring for anomalous behavior is implemented. Describe any tools used specifically to manage privileged accounts (e.g., firecall access controls).	- 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-03	DE.CM-03.03

FS SSG.127	**Third-party connection authorization:** The organization reviews, documents, authorizes, and monitors all third-party connections, data transfer mechanisms, and Application Programming Interfaces (APIs).	--	--	**Yes**	The organization should have a process for documenting, reviewing, and approving external connections, reviewing, and approving external connections, data transfer, and APIs to ensure that appropriate security and resilience design is in place. Organizations should establish ongoing monitoring requirements to control and monitor all third-party connections, data transfer mechanisms, and application programming interfaces (APIs). Controls may include network segmentation, in-line intrusion detection systems/intrusion prevention systems, security information and event management (SIEM), or log aggregation tools, among others. There should be evidence that each third-party service has been formally approved (e.g., through signed contracts and Board meeting minutes). Further, back up connections should be tested to ensure resiliency and limit outage risk. Describe how the organization reviews, documents, authorizes, and monitors all third-party connections, data transfer mechanisms, and APIs. Provide information regarding the process. Provide information of related policies, standards, and processes.	- Third-party policies, standards, and processes - Third-party contracts and other approvals (e.g., Board meeting minutes) - Inventory of third-parties and any related reporting - Risk assessment programs/processes - Network diagrams identifying all external connections to third-parties - Use cases - List of related tools for monitoring third parties to detect potential cybersecurity events - Connections, data transfer, API design documentation	DE.CM-06	DE.CM-06.01
FS SSG.128	**Third-party access monitoring:** 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.	--	--	**Yes**	Appropriate access controls and monitoring should be in place between the organization and service provider systems and employees. The organization should have procedures in place detailing specific activities that are authorized by third-party service providers and systems which monitor and alert on unauthorized activity. Describe what the organization has implemented with regards to explicit approval and logging processes and alerts to monitor and prevent any unauthorized access to a critical system by a third-party service provider.	- 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-06	DE.CM-06.02
FS SSG.129	**Unauthorized software, hardware, or configuration changes:** The organization has policies, procedures, and tools in place to monitor for, detect, and block the use of unsupported or unauthorized software, hardware, or configuration changes.	**3.P**	**Yes**	**Yes**	Unauthorized software, hardware, or configuration changes introduces significant risk to the organization, as actors can gain access to sensitive data. The organization should implement controls to monitor, scan, detect, and block unauthorized changes to protect integrity of software, hardware, and firmware. Unsupported operating systems and components also may introduce significant risk to the organization, as updates, patches and fixes are no longer available. The organization should implement compensating controls to protect against the threats of unsupported systems. Describe what policies, procedures, and tools have been implemented to monitor, detect, and/or block the use of unsupported and unauthorized software, hardware, or configuration changes. Provide information on the configuration, software, and hardware management processes.	- Unsupported and unauthorized software, hardware, configuration change identification/review process and reports - Configuration management policies, standards, and processes - Software management policies, standards, and processes - Hardware management policies, standards, and procedures - Proof that related tools for preventing, monitoring, and remediating of unauthorized software, hardware, configuration are in place - Supported software, hardware, configuration changes - Documentation that programs that can override system, object, network, virtual machine and application controls are restricted	DE.CM-09	DE.CM-09.03

FS SSG.130	**Alert parameters and thresholds:** The organization establishes, documents, and regularly reviews event alert parameters and thresholds, as well as rule-based triggers to support automated responses, when known attack patterns, signatures or behaviors are detected.	**4.B**	**Yes**	**Yes**	Conditions to scan for in log data should be defined to alert on potentially adverse events. Parameters or thresholds should be established to provide alerts and notifications to the proper personnel when those thresholds are exceeded. For example, an exception report can be used to document when a threshold has been exceeded. Describe how the organization establishes, documents, and regularly reviews event alert parameters and thresholds, as well as rule-based triggers to support automated responses, when known attack patterns, signatures or behaviors are detected.	- Security information and event management (SIEM) documentation - Documents on methods in place for monitoring across the environment to detect anomalous activities - Documents on mechanisms or tools in place to alert management (e.g., detection methods and searches, automated playbooks, etc.) - Documents showing that incident alert parameters and thresholds are established - Examples of third-party alert procedures/agreements with critical service providers - Related reporting - Documents showing that alert parameters are set for detecting information security incidents that prompt mitigating actions - System performance reports contain information that can be used as a risk indicator to detect information security incidents	DE.AE-02	DE.AE-02.02
FS SSG.131	**Infrastructure monitoring:** The organization implements systematic and real-time logging, collection, monitoring, detection, and alerting measures across multiple layers of the organization's infrastructure, including physical perimeters, network, operating systems, applications, data, and external (cloud and outsourced) environments, sufficient to protect the organization's information assets.	**4.B**	**Yes**	**Yes**	Protecting organizations from cyber threats requires constant vigilance over security infrastructure and critical information assets. Real time or near real-time security logs and alerts help identify and thwart malicious activity. Systems must balance numerous ongoing operational and strategic security tasks. The organization should implement device and network monitoring technologies that provide actionable information to inform and support incident response. Organizations should also monitor the physical environment (e.g., entrances, restricted areas, confidential data repositories, vault areas, ATMs, etc.). Describe how the organization has implemented systematic and real-time/near real-time logging, collection monitoring, detection, and alerting measures across multiple layers of the organization's infrastructure and external environments, that produce actionable information sufficient to protect the organization's information assets. Describe the methodology and tools utilized to cover physical perimeters, network, operating systems, applications, and data.	- Event logging, monitoring, detecting, and alerting methodology - Examples of event logging - Documentation of the monitoring of logs and ports - Documents on mechanisms and tools in place to alert management to potential attacks (e.g., antivirus alerts, log event alerts) and trigger the incident response program - Related reporting - Documents showing the physical environment is monitored to detect potential unauthorized access - System performance reports containing information that can be used as a risk indicator to detect an information security incident	DE.AE-03	DE.AE-03.01
FS SSG.132	**Event aggregation, correlation, and analysis:** The organization performs real-time central analysis, aggregation, and correlation of anomalous activities, network and system alerts, and relevant event and cyber threat intelligence, including both internal and external (cloud and outsourced) environments, to better detect and prevent multifaceted cyber attacks.	**4.B**	**Yes**	**Yes**	The organization should deploy tools, as appropriate, to collect and aggregate information, including threat intelligence, to provide a holistic view of the organization's security posture. The organization should monitor network traffic in real-time with automated tools in order to detect internal and external cyber threats. For example, a security information and event management (SIEM) tool can be used to collect and log security-related documentation for analysis and correlation. Describe the tools utilized to perform real-time central analysis, aggregation, and correlation of anomalous activities, network and system alerts, and relevant event and cyber threat intelligence from multiple sources, including both internal and external sources, to better detect and prevent multifaceted cyber-attacks.	- 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-03	DE.AE-03.02

FS SSG.133	**Event triage:** The organization has a documented process to analyze and triage incidents to assess root cause, technical impact, mitigation priority, and business impact on the organization, as well as across the financial sector and other third party stakeholders.	**4.B**	**Yes**	**Yes**	The organization should have processes in place for analyzing the impact associated with cybersecurity incidents. The significance of cybersecurity risks depends upon their nature, extent, potential magnitude, and the range of harm such incidents could cause to the organization's reputation, financial performance, customer relations, and impact across the financial sector. Describe the documented process to analyze and triage incidents to assess root cause, technical impact, mitigation priority, the impact of a significant cybersecurity incident, as defined by the organization's risk appetite. Describe how the process for the organization to analyze and triage considering the financial impact across the financial sector, as appropriate, per the organization's size, scope, complexity, and role in the financial sector. Provide information on the organization's defined and established incident thresholds. Describe the documented process in place to analyze and triage incidents based on the potential business impact on other third party stakeholders.	- 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	DE.AE-04	DE.AE-04.01
FS SSG.134	**Event alerting:** The organization has established processes and protocols to communicate, alert, and regularly report potential cyber attacks and incident information, including its corresponding analysis and cyber threat intelligence, to authorized internal and external stakeholders.	**4.B, 5.B**	**Yes**	**Yes**	Organizations should stay aware of highly visible cyber events through open-source reporting, industry alerts, law enforcement alerts, or regulatory alerts. The organization's management should have processes in place for periodically reporting incident information within the organization, to staff, management, and the Board. The organization should also have processes in place for sharing threat and incident data with external stakeholders (e.g., clients, regulators, law enforcement, etc.) to benefit the financial sector by enabling other organizations to assess and respond to current attacks. Describe the established processes and escalation protocols to communicate, alert and regularly report potential cyber attacks and incident information, including the corresponding analysis and cyber threat intelligence, to authorized internal and external stakeholders.	- Security incident response policies, standards, and procedures addressing the concepts of threat information sharing - Related policies, standards, and procedures for reacting and responding to cyber incidents - Cybersecurity incident response plan example - Event/incident escalation procedures and triage process - Proof of threat intelligence collection, correlation, and dissemination process and reporting - Related reporting and alert examples - Use cases - Board or board subcommittee meeting minutes showing newsworthy cyber events or regulatory alerts are addressed. - Information security threats and materials gathered and shared with applicable employees - Proof of threat information shared with law enforcement and regulators	DE.AE-06	DE.AE-06.01

RESPOND								
FS SSG.135	**Response plan execution:** The organization's response plans are in place and executed during or after an incident, to include coordination with relevant third parties and engagement of third-party incident support services.	--	**Yes**	**Yes**	The organization should have incident response policies and plans that properly work in concert with business continuity plans and should execute such plans during or after identifying an incident. Responses should describe how the organization's response plans are established, maintained, and executed during or after an incident, including coordination with relevant third parties and engagement of third-party incident support services. Provide information on the structure and process. Refer to ID.IM-04.08, how the organization's response plans are updated and improved based on cyber threat intelligence and lessons learned.	- Security incident response policies, standards, and procedures - Cybersecurity incident response plan example - Playbooks or other incident response related plans and processes	RS.MA-01	RS.MA-01.01
FS SSG.136	**Reliable event detection and analysis:** Tools and processes are in place to ensure timely detection, inspection, assessment, and analysis of security event data for reliable activation of incident response processes.	--	**Yes**	**Yes**	The most effective way to detect and prevent network compromise and data breaches is through early recognition and investigation of potentially suspicious network activity. The organization may use active and/or passive monitoring tools and processes to detect any deviations from normal or expected operations (i.e., network-monitoring software, logging, detection solutions, etc.). Responses should describe the tools and processes that are in place to ensure timely detection, inspection, assessment, and analysis of the security event data for reliable activation of incident response processes.	- Security incident response policies, standards, and procedures - Incident response examples or playbooks - Security logging and monitoring policy, standard, and procedure - Related security logging and monitoring tools - Logging and Monitoring use cases - Alerting use cases and thresholds - Logging and reporting examples - Related assessment reporting	RS.MA-02	RS.MA-02.01
FS SSG.137	**Incident severity levels and escalation:** The organization's incident response plans define severity levels and associated criteria for initiating response plans and escalating event response to appropriate stakeholders and management levels.	--	--	**Yes**	The incident response plans should include related information on the incident's severity levels, and communications plans. The response plans should operate with the authority to collect and document information on the incident, assess risk, implement mitigation strategies, escalate issues when necessary, and consider any necessary changes to business practices. Provide information on how the organization's incident response plan defines severity levels and associated criteria for initiating response plans. Describe reporting and escalation processes to the appropriate stakeholders and management levels.	- 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.MA-05	RS.MA-05.01
FS SSG.138	**Incident investigation and root cause determination:** The organization performs a thorough investigation to determine the nature and scope of an event, possible root causes, and the potential damage inflicted.	--	**Yes**	**Yes**	The organization should review the impact of the cybersecurity incident, as analyzing the impact helps organizations align and prioritize resources to risks. Describe how the organization performs thorough investigations in order to determine the nature and scope of an event, possible root causes, and the potential damage inflicted. Provide information on any functional teams in place and their roles and responsibilities. Functional teams may include forensics and root cause analysis teams, among others.	- 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-03	RS.AN-03.01
FS SSG.139	**Incident impact analysis:** Available incident information is assessed to determine the extent of impact to the organization and its stakeholders, the potential near- and long-term financial implications, and whether or not the incident constitutes a material event.	--	**Yes**	**Yes**	Organizations should have policies, standards, and processes in place to assess the impact associated with cybersecurity incidents. As referenced in DE.AE-04.01, the impact should be determined based upon their nature, extent, potential magnitude, and the range of harm such incidents could cause to the organization's reputation, financial performance, customer relations, and impact across the financial sector. The organization must determine if an incident constitutes a material event to the company and its stakeholders, which has regularly reporting implications. Such determinations should be made at the most senior levels of a company, and with the advice of legal counsel and the Chief Information Security Office. Describe how available incident information is assessed to determine the extent of impact to the organization and its stakeholders, the potential near- and long-term financial implications, and the determination of incident materiality.	- 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	RS.AN-08	RS.AN-08.01

FS SSG.140	**Incident escalation protocols:** The organization's incident response program includes defined and approved escalation protocols, linked to organizational decision levels and communication strategies, including which types of information will be shared, with whom (e.g., the organization's governing authority and senior management), and how information provided to the organization will be acted upon.	**5.A**	**Yes**	**Yes**	The organization's incident response plan should specify which incidents must be reported, when they must be reported, and to whom based on the severity level of the incident. Parties commonly notified of cyber incidents include the CIO, head of information security, local information security officer, legal counsel, other incident response teams, and system owners, among others. Describe how the organization's incident response program includes defined and approved escalation protocols, linked to organizational decision levels and communication strategies, including which types of information will be shared, with whom (e.g., the organization's appropriate governing authority and senior management), and how information provided to the organization will be acted upon. Focus evidence on escalation protocols and related processes, based on the severity level of the incident.	- Security incident response policies, standards, and procedures - Incident response examples or playbooks - Related notification procedures - Related documentation and examples - Information classification and handling guidelines	RS.CO-02	RS.CO-02.01
FS SSG.141	**Incident notification and reporting:** In the event of an incident, the organization notifies impacted stakeholders including, as required, government bodies, self-regulatory agencies and/or other supervisory bodies, within required timeframes.	**5.A, 5.B**	**Yes**	**Yes**	The incident response program should include reporting procedures to ensure that the organization promptly reports incident information to appropriate authorities, such as primary regulators and law enforcement. The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, directives, policies, regulations, standards and guidance. Describe the process the organization utilizes to notify impacted stakeholders including, as required, government bodies, self-regulatory agencies or any other supervisory bodies in the event of an incident. Provide information with a focus on stakeholders. If an incident is determined to be a material event, in the U.S., required SEC regulatory filings must be made. Describe how the organization notifies impacted stakeholders within required timeframes.	- Security incident response policies, standards, and procedures - Incident response examples or playbooks - Related notification procedures - Related documentation and examples	RS.CO-02	RS.CO-02.02
FS SSG.142	**Incident response communication procedures:** The organization maintains and regularly tests incident response communication procedures, with associated contact lists, call trees, and automatic notifications, to quickly coordinate and communicate with internal and external stakeholders during or following an incident.	**5.A**	**Yes**	**Yes**	The organization should have policies and procedures for communicating cyber and operational incidents to internal and external stakeholders. Internal communication can occur through various methods, including communicational channels, building out contact lists, automatic notifications, among others. Testing should be performed on incident response communication procedures to ensure timely response of incidents. Describe testing regularly performed on incident response communication procedures to quickly coordinate and communicate with internal and external stakeholders during or following an incident. Provide information on the communications plan activities (e.g., associated contact lists, call trees, and automated notification tools).	- Security incident response policies, standards, and procedures - Incident response examples or playbooks - Incident response process, major incident management process, or other related notification procedures - Cyber threat/incident information sharing examples - Related testing of incident response communications - Communication plan activities - Automated notification tools in use	RS.CO-02	RS.CO-02.03

FS SSG.143	**Incident intelligence sharing:** In the event of an incident, the organization shares authorized information, in a defined manner and through trusted channels, to facilitate the detection, response, resumption and recovery of its own systems and those of other partners and critical sector participants.	**5.A, 5.B**	**Yes**	**Yes**	The organization should actively participate in information sharing organizations (i.e., the Analysis and Resilience Center for Systemic Risk (ARC), FS-ISAC, industry associations) to receive and provide external threat and vulnerability information. The organization can also establish threat intelligence sharing relationships directly with peer organizations. To protect the confidentiality and the integrity of the information, organizations should have formal information sharing agreements that document the nature of the information being shared, handling and storage, ownership, retention, and related matters. Describe how the organization actively participates in multilateral information-sharing arrangements to facilitate a sector-wide response to large-scale incidents. Provide information related to the sector-wide information sharing. Describe how information is shared consistent with response plans. Describe how the organization shares authorized information, in a defined manner and through trusted channels, to facilitate the detection, response, resumption and recovery of its own systems and those of other partners and critical sector participants.	- 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-03	RS.CO-03.02
FS SSG.144	**Incident containment:** The organization has established processes to implement vulnerability mitigation plans, involve third-party partners and outside expertise as needed, and contain incidents in a timely manner.	--	**Yes**	**Yes**	Describe the established processes to implement vulnerability mitigation plans, as well as validate their completion and effectiveness. Describe how the organization mitigates cybersecurity incidents in a timely manner. Provide examples. Provide information on how mitigation plans are reviewed and agreed upon with business stakeholders. Provide information on how remediation is tested and verified.	- Vulnerability management security standard - Remediation management documentation - Related examples - Related reporting	RS.MI-01	RS.MI-01.01
FS SSG.145	**Incident vulnerability remediation:** Targeted investigations and actions are taken to ensure that all vulnerabilities, system components, devices, or remnants used or leveraged in an attack (e.g., malware, compromised accounts, open ports, etc.) are removed or otherwise returned to a secure and reliable state, or that plans to address the vulnerabilities are documented.	--	**Yes**	**Yes**	Organizations should have strategies and procedures for mitigation and eradication in place for a timely containment of vulnerabilities. Describe eradication processes in place. Describe how targeted investigations determine root causes of incidents and provide actionable results to ensure that all vulnerabilities are removed or otherwise returned to a secure and reliable state. Describe target investigations and actions taken to ensure that all vulnerabilities, system components, devices, or remnants used or leveraged in an action are removed or otherwise returned to a secure and reliable state. Provide information of documented plans to address the identified vulnerabilities.	- Vulnerability management security standard - Incident response policies, standards, and plans - Remediation management documentation - Related examples - Related reporting	RS.MI-02	RS.MI-02.01

RECOVER								
FS SSG.146	**Recovery plan execution:** The organization executes its recovery plans, including incident recovery, disaster recovery, and business continuity plans, during or after an incident to resume operations.	**6.A**	**Yes**	**Yes**	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.	- Security incident response policy, standard, procedures - Incident response examples or playbooks - Business continuity/resilience policy, standard, and procedures - Data backup and recovery policy, standard, and procedures - Disaster recovery plans	RC.RP-01	RC.RP-01.01
FS SSG.147	**Recovery prioritization:** Recovery plans are executed by first resuming critical services and core business functions, while minimizing any potential concurrent and widespread interruptions to interconnected entities and critical infrastructure, such as energy and telecommunications.	**6.A**	**Yes**	**Yes**	A formal backup and recovery plan describes how critical systems are backed up and restored in the event of loss or corruption of production data. The organization should have a process in place to conduct business impact analysis to identify criticality. Describe how recovery plans are executed by first resuming critical services and core business functions within a defined timeframe. Describe how the plans could be executed while minimizing any potential concurrent and widespread interruptions to interconnected entities and critical infrastructure, such as energy and telecommunications (e.g., how recovery plans include communication plans with interconnected entities).	- Business continuity/resilience policy, standard, and procedures - Data center recovery procedures - Business recovery procedures - Other related recovery procedures	RC.RP-02	RC.RP-02.02
FS SSG.148	**Incident closure:** Incident management activities are closed under defined conditions and documentation to support subsequent post-mortem review, process improvement, and any follow-on activities is collected and verified.	**6.A**	**Yes**	**Yes**	Organizations should have processes for post-incident analysis to evaluate the incident response process, discuss identified gaps, minimize future impact, and discuss the closure of the relevant incident. Provide information on applicable internal and external stakeholders involved. Provide information on how the organization's establishes defined conditions and documentation to provide closure of incident management activities. Provide information of the subsequent post-mortem review. Describe how the post-incident process drives process improvements and incorporate lessons learned. Describe how the organization collects and verifies any follow-on activities needed for the closure of incident management activities.	- Business continuity/resilience policy, standard, and procedures - Post-incident analysis - Documentation of process improvements - Relevant meeting notes - Data center recovery procedures - Business recovery procedures - Service continuity planning standards and procedures - Recovery time objectives for critical systems - Other related recovery procedures	RC.RP-06	RC.RP-06.01
FS SSG.149	**Recovery activity external communications:** The organization promptly communicates the status of recovery activities to regulatory authorities and relevant external stakeholders, as required or appropriate.	**--**	**Yes**	**Yes**	Proactively sharing threat intelligence helps organizations achieve broader cybersecurity situational awareness among internal and external stakeholders. Describe how the status of recovery activities is promptly communicated to regulatory authorities and relevant external stakeholders, as required or appropriate.	- 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-03	RC.CO-03.02

	EXTEND							
FS SSG.150	**Due diligence resource allocation:** The organization implements procedures, and allocates sufficient resources with the requisite knowledge and experience, to conduct third party due diligence and risk assessment consistent with the procurement plan and commensurate with level of risk, criticality, and complexity of each third-party relationship.	**1.E**	**Yes**	**Yes**	The organization should establish formal procedures to establish, manage, and monitor its third party relationships commensurate with the risk each third party poses to the organization. Organizations should allocate resources with the requisite knowledge and experience to manage ongoing third party risks. Procedures should establish processes for conducting third party due diligence and risk assessment consistent with the procurement plan. Describe how the organization allocates sufficient resources with the requisite knowledge and experience to conduct due diligence and manage and monitor its third party relationships. Describe how the organization establishes procedures to conduct third party due diligence and risk assessment consistent with the procurement plan and commensurate with the level of risk, criticality, and complexity of each third party relationship.	- Third-party security policy, standard, and procedures - Third-party risk management program - Contract with third parties - Procurement plans - Risk assessments - Third-party risk management governance roles and responsibilities - Due diligence policy, requirement, or questionnaire - Other related third-party assessment processes, examples, and reporting	GV.SC-06	EX.DD-02.01
FS SSG.151	**Third-party business profile due diligence:** The organization reviews and evaluates documentation, such as financial statements, independent audit reports, pooled/shared assessments, control test reports, SEC filings, and past and pending litigation, to the extent required to determine a prospective critical third party's soundness as a business and the quality and sustainability of its internal controls.	--	--	**Yes**	Organizations should determine a prospective critical third party's soundness by performing due diligence and reviewing and evaluating documentation, such as financial statements, independent audit reports, pooled/shared assessments, control test reports, SEC, filings, and past and pending litigation. High-risk vendors may necessitate a more frequent level of review. The organization's contracts with third parties should stipulate requirements for reviews, frequency of reviews, and required documentation to be provided. Describe how the organization reviews and evaluates documentation to the extent required to determine a prospective critical third party's soundness as a business and the quality and sustainability of its internal controls.	- Third-party security policy, standard, and procedures - Third-party risk management program - Documented processes to review and evaluate documentation of a prospective critical third party - Contract with third parties - Procurement plans - Risk assessments - Third-party risk management governance roles and responsibilities - Due diligence policy, requirement, or questionnaire - Other related third-party assessment processes, examples, and reporting	GV.SC-06	EX.DD-02.03
FS SSG.152	**Third-party internal controls due diligence:** The organization reviews and assesses the prospective third party's controls for managing its suppliers and subcontractors (fourth and nth parties), any proposed role fourth and nth parties will play in delivering the products or services, and any specific fourth- and nth-party controls or alternative arrangements the organization may require to protect its interests.	--	--	**Yes**	Critical vendors often have third-party relationships that can present risk to their clients if not properly managed. These vendors should have effective third-party risk management programs and controls in place and appropriate methods for demonstrating due diligence over their third-party relationships. Provide information on the process in place and used to confirm that the organization's third-party service providers conduct due diligence of their own third parties (e.g., subcontractors). Describe how the organization reviews and assesses any proposed role fourth and nth parties will pay in delivering the products and services, and any specific fourth- and nth-party controls or alternative arrangements the organization may require to protect its interests.	- 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	GV.SC-06	EX.DD-02.04

FS SSG.153	**Third-party cybersecurity program due diligence:** The organization reviews, evaluates, and risk assesses a prospective critical third party's cybersecurity program, including its ability to identify, assess, monitor, and mitigate its cyber risks; the completeness of its policies and procedures; the strength of its technical and administrative controls; and the coverage of its internal and independent control testing programs.	**1.E**	**Yes**	**Yes**	The organization's management may rely on third parties to provide critical services; however, management remains responsible for ensuring the confidentiality, integrity, and availability of the organization's systems and information. The organization's third parties should be required to follow minimum cybersecurity requirements that meet the required cybersecurity practices of the organization. Procurement due diligence should review and evaluate the effectiveness of a prospective critical third party's cybersecurity program before establishing a relationship. Describe how the organization reviews and evaluates a prospective critical third party's cybersecurity program. Provide information on how the organization evaluates a critical third party's ability to identify, assess, monitor, and mitigate its cyber risks. Describe how the organization evaluates a critical third party's completeness of policies and procedures, and strength of their technical and administrative controls. Provide information on how the organization evaluates the coverage of a critical third party's internal and independent control testing programs. Describe the documentation, questionnaire, and other information sources used to evaluate vendor security programs.	- Third-party security policy, standard, and procedures - Third-party risk management program - Contract with third parties, including no delegation clause or equivalent - Risk assessments that third parties have conducted of subcontractors - Related third-party reporting - Third-party risk management governance roles and responsibilities - Due diligence policy, requirement, or questionnaire - Other related third-party assessment processes, examples, and reporting - Third party due diligence questionnaires	ID.RA-10	EX.DD-03.01
FS SSG.154	**Third-party business continuity program due diligence:** The organization reviews, evaluates, and risk assesses a prospective critical third party's business continuity program, to include business impact analyses, risk assessments, continuity plans, disaster recovery plans, technology resilience architecture, and response and recovery plans, test plans, and test results.	--	--	**Yes**	Business disruptions to the third party could pose a risk to the organization and may affect the organization's ability to service clients. Organizations should ensure that a prospective critical third party has a business continuity program in place. Describe how the organization reviews and evaluates a prospective critical third party's business continuity program. Provide information on how the organization evaluates a critical third party's business continuity processes, including business impact analyses, risk assessments, and program testing. Provide information on how the organization evaluates a critical third party's business continuity plans, including, disaster recovery plans, technology resilience architecture, and response and recovery plans, test plans, and test results.	- Inventory of critical external dependencies and business functions - Identification criteria of critical external dependencies and related business functions - Third-party security policy, standard, and procedures - Third-party risk management program - Critical third-party reporting or other related reporting - Contract reporting - Third-party risk management governance roles and responsibilities - Due diligence policy, requirement, or questionnaire - Other related third-party assessment processes, examples, and reporting	ID.RA-10	EX.DD-03.02
FS SSG.155	**Third-party incident response program due diligence:** The organization review, evaluates, and risk assesses a prospective critical third party's incident response program, to include monitoring and alerting capabilities, incident reporting procedures and protocols, and capabilities for event analysis, problem resolution, and forensic investigation.	--	--	**Yes**	Incidents that occur within a third party could pose a risk to the organization and may affect the organization's ability to service clients. Organizations should ensure that a prospective critical third party has a robust incident response program in place. Describe how the organization reviews and evaluates a prospective critical third party's incident response program, to include monitoring and alerting capabilities, incident reporting procedures and protocols, and capabilities for event analysis, problem resolution, and forensic investigation.	- Third-party security policy, standard, and procedures - Third-party risk management program - Contract with third parties, including no delegation clause or equivalent - Risk assessments that third parties have conducted of subcontractors - Related third-party reporting - Third-party risk management governance roles and responsibilities - Due diligence policy, requirement, or questionnaire - Other related third-party assessment processes, examples, and reporting	ID.RA-10	EX.DD-03.03

FS SSG.156	**Third-party systems and software evaluation:** The organization defines and implements procedures for assessing the compatibility, security, integrity, and authenticity of externally-developed or externally-sourced applications, software, software components, and firmware before deployment and upon any major change.	**1.E**	**Yes**	**Yes**	The organization's management should establish a formal process and/or procedures for evaluating externally developed or externally-sourced applications before deployment and upon any major change. Provide information on the processes used within the organization to evaluate (e.g., assessing or testing) the compatibility, security, and integrity. Provide information on the processes used within the organization to evaluate the authenticity of externally-developed or externally-sourced applications, software, software components, and firmware before deployment and upon any major change.	- 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	ID.RA-09	EX.DD-04.01
FS SSG.157	**Third-party contracts:** Contracts with suppliers clearly detail the general terms, nature, and scope of the arrangement, to include the distribution of responsibilities between the parties; costs, compensation, reimbursements, incentives, and penalties; service level agreements, performance measures, and benchmarks; responsibilities for providing, receiving, and retaining information; recourse provisions; and the organization's rights to review, monitor, and audit the supplier's activities.	**1.E**	**Yes**	**Yes**	The organization should have documented minimum contract requirements for third parties. Describe the organization's process for developing and negotiating contracts with suppliers. Provide information on how the organization creates contracts that clearly details the general terms, nature, and scope of the arrangement. Contracts should include the distribution of roles and responsibilities between parties. Provide information on the contract's documentation of cost, compensation, reimbursement, incentives, and penalties. Describe how the organization outlines service level agreements, performance measures, and benchmarks. Provide information on the contract outlining responsibilities for providing, receiving, and retaining information, as well as recourse provisions, and the organization's rights to review, monitor, and audit the supplier's activities. The organization's management should consider including termination rights and recourse within contracts for a variety of conditions, including failure to meet cybersecurity requirements.	- Contract guidance - Contract clauses - Contract reporting - Template/standard contract clauses and terms - Procurement and contracting policies and procedures	GV.SC-05	EX.CN-01.01
FS SSG.158	**Third-party management of suppliers:** Contracts with suppliers address, as relevant to the product or service, the supplier's requirements for managing its own suppliers and partners (fourth parties) and the risks those fourth parties may pose to the third party and to the organization, to include fourth party due diligence, limitations on activities or geography, monitoring, notifications, liability and indemnifications, etc.	--	--	**Yes**	Management must require third-party service providers by contract to manage their own suppliers and partners. Suppliers should have risk management processes, plans, and strategies in place to mitigate risks that those fourth parties may post to the third party. Organizations should maintain a third party risk management program that considers risks that fourth parties may impose on the organization. Describe how the organization's contracts require suppliers to manage their own suppliers and partners (fourth parties) and maintain those practices for the life of the relationship. Describe how the organization ensures that suppliers are performing fourth party due diligence, and considering limitations on activities, or geography. Describe how the organizations ensures that supplies have processes for monitoring, notifications, liability, and indemnifications of a fourth party.	- 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	GV.SC-05	EX.CN-01.02
FS SSG.159	**Third-party cybersecurity requirements:** The organization's contracts require third-parties to implement minimum technology and cybersecurity management requirements, to maintain those practices for the life of the relationship, and to provide evidence of compliance on an ongoing basis.	**1.E**	**Yes**	**Yes**	Management should require third-party service providers, by contract, to implement appropriate measures designed to meet the organization's minimum cybersecurity requirements and the objectives of regulatory guidelines. Contract clauses should include the organization's right to audit a supplier's activities throughout the relationship, service level agreements, performance measures, timely notification of any security breaches, among others. Organizations should establish an acceptable template contract with consistent clauses that can be used for all third parties. Describe how the organization's contracts require third parties to implement minimum cybersecurity requirements and to maintain those practices for the life of the relationship. Organizations may need to maintain cybersecurity requirements after the relationship ends (e.g., return of data, escalate the receipt of sensitive data). Describe how contracts address any cybersecurity requirements that extend beyond the relationship with the organization.	- 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 - Template/standard contract clauses and terms	GV.SC-05	EX.CN-02.01

FS SSG.160	**Third-party incident and vulnerability notification requirements:** Minimum cybersecurity requirements for third-parties include requirements for incident and vulnerability notification, to include the types of events requiring notification, notification timeframes, and escalation protocols.	**1.D**	**Yes**	**Yes**	The organization's management may rely on third parties to provide critical services; however, management remains responsible for ensuring the confidentiality, integrity, and availability of the organization's systems and information. The organization's third parties should be required to follow minimum cybersecurity requirements that meet the cybersecurity practices of the organization, including requirements for incident and vulnerability notification. These requirements may be documented within service contracts, Requests for Proposals (RFP), and/or other reporting. Describe the documented minimum cybersecurity requirements for third parties that meet, at a minimum, the cybersecurity practices of the organization. Describe reporting requirements for events requiring notification, escalation protocols and coordination mechanisms. Describe the documented notification timeframes.	- Third-party security policy, standard, and procedures - Third-party risk management program - Third-party cybersecurity requirements and related controls - Contractual language on security requirements (security schedule) - RFPs or RFIs documenting minimum cybersecurity requirements - Related third-party reporting	GV.SC-05	EX.CN-02.02
FS SSG.161	**Third-party business continuity program requirements:** Contracts with suppliers address, as relevant to the product or service, the supplier's obligation to maintain and regularly test a business continuity program and disaster recovery capability the meets the defined resilience requirements of the organization.	--	--	**Yes**	Management should require third-party service providers by contract to maintain and regularly test a business continuity program and disaster recovery capability designed to meet the organization's defined resilience requirements. Describe how the organization's contracts require suppliers to implement a business continuity program and discovery recovery capability and maintain those practices for the life of the relationship. Describe how contracts address the supplier's obligation to regularly test their business continuity program and discovery recovery capabilityManagement should require third-party service providers by contract to maintain and regularly test a business continuity program and disaster recovery capability designed to meet the organization's defined resilience requirements. Describe how the organization's contracts require suppliers to implement a business continuity program and discovery recovery capability and maintain those practices for the life of the relationship. Describe how contracts address the supplier's obligation to regularly test their business continuity program and discovery recovery capability.	- Third-party security policy, standard, and procedures - Third-party risk management program - Third-party cybersecurity requirements and related controls - Contractual language on security requirements (security schedule) - Examples of contracts with third parties - Related testing of business continuity program and disaster recovery capability	GV.SC-05	EX.CN-02.03
FS SSG.162	**Third-party monitoring and management resources:** The organization implements procedures, and allocates sufficient resources with the requisite knowledge and experience, to manage and monitor its third-party relationships to a degree and extent commensurate with the risk each third party poses to the organization and the criticality of the third party's products, services, and/or relationship to the organization.	**1.E**	**Yes**	**Yes**	The organization should conduct ongoing monitoring on all potential third parties before selecting and entering into contracts or relationships with third parties. Organizations should establish a formal third-party risk management program aligned to the organization's risk management program. Describe how the organization allocates resources with the requisite knowledge and experience to manage ongoing third party risks. Describe how the organization determines the criticality of the third party's products, services, and/or relationship to the organization. Describe documented procedures established to manage and monitor third-party relationships commensurate with the risk each third party poses to the organization.	- Third-party security policy, standard, and procedures - Third-party risk management program - Contract guidance - Contract reporting - Monitoring processes and reporting - Related third-party reporting	GV.SC-07	EX.MM-01.01
FS SSG.163	**Third-party supplier management monitoring:** The organization regularly assesses a critical third party's program and ability to manage its own suppliers and partners (fourth and nth parties) and the risks those fourth and nth parties may pose to the third party and to the organization (e.g., cybersecurity supply chain risk, concentration risk, reputation risk, foreign-party risk, etc.)	--	--	**Yes**	As referenced in EX.CN-02.02, the organization has documented minimum cybersecurity requirements for third parties. Third-party risk management plans should have processes to regularly assess a critical third party's program and ability to manage its own suppliers and partners. Organizations should ensure there is visibility with third parties to assess risks of fourth and nth parties. Inherent risks should be assessed within the organization's established risk appetite. Describe how the organization regularly assess a critical third party's program and ability to manage its own suppliers and partners. Provide information of continuous monitoring performed on suppliers to understand risk exposure.	- Third-party security policy, standard, and procedures - Third-party risk management program - Contract guidance - Contractual language on security requirements (security schedule) - Contract clauses, including audit rights - Contract reporting - Monitoring plans - Related third-party reporting - Risk assessments that third parties have conducted of subcontractors	GV.SC-07	EX.MM-01.05

FS SSG.164	**Third-party security program monitoring:** The organization conducts regular third-party reviews for critical vendors to validate that requisite security and contractual controls are in place and continue to be operating as expected.	**1.E**	**Yes**	**Yes**	The organization may rely on third parties to provide critical services; however, management remains responsible for overseeing the effectiveness of the services provided by third-party service providers. High-risk vendors may necessitate a more frequent and detailed level of review. The organization may employ third party services that monitor the security posture of critical third parties. Third-party reviews may include audits, operational performance reports, financial condition, or other assessments. The organization's contracts with third parties should stipulate requirements for reviews, frequency of reviews, and required documentation. Describe how the organization conducts regular third-party reviews for critical vendors to validate that requisite and contractual controls have been implemented and continue to be operating as expected. Provide information on how the organization tracks results of regular third-party reviews for critical vendors within the organization.	- Third-party security policy, standard, and procedures - Third-party risk management program - Critical third-party identification procedures - Critical third-party reporting - Audit reports - Contracts clauses, including audit rights - Related third-party reporting - Security monitoring reports	GV.SC-07	EX.MM-02.01
FS SSG.165	**Third-party business continuity program monitoring:** A process is in place to confirm that the organization's critical third-party service providers maintain their business continuity programs, conduct regular resiliency testing, and participate in joint and/or bilateral recovery exercises and tests.	--	--	**Yes**	The organization's third-party oversight should include reviewing third parties' business continuity programs, resilience plans, and testing. The organization's management may also actively participate in joint and/or bilateral recovery exercises and tests. Provide information on the process in place used to confirm that the organization's critical third-party service providers maintain their business continuity programs. Describe the process in place to confirm that regular resiliency testing is conducted by third parties. Responses should include participation from third parties in joint and/or bilateral recovery exercises and tests.	- Third-party security policy, standard, and procedures - Third-party risk management program - Contract guidance - Contract reporting - Related third-party reporting	GV.SC-07	EX.MM-02.02
FS SSG.166	**Third-party security improvement collaboration:** The organization collaborates with suppliers to maintain and improve the secure use of products, services, and external connections.	--	--	**Yes**	Describe how the organization collaborates with suppliers (e.g., core processing, online and mobile banking, settlement activities, disaster recovery services, cloud service providers) to maintain and improve the security of products, services, and external connections. Hardware and software vendors may periodically update recommended security settings and configurations, especially when updated product versions are released. Examples include requiring each vendor to use a single remote access solution, ensuring that vendors do not share credentials, multifactor authentication, and enforcing the concept of least access or privilege.	- 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	GV.SC-07	EX.MM-02.03
FS SSG.167	**Third-party relationship termination:** Upon termination of a third-party agreement, the organization ensures that all technical and security matters (access, connections, etc.), business matters (service, support, and ongoing relationship), property matters (data, physical, and intellectual), and legal matters are addressed in a timely manner.	**1.E**	**Yes**	**Yes**	Organizations should have plans and processes in place for termination of third-party agreements. Provide information of documented exit strategies commensurate with the risk of the third party. Contracts should detail notification requirements and time frames to address unresolved matters. Describe how the organization ensures that all technical, security, business, property, and legal matters are addressed in a timely manner upon termination of a third-party agreement. Provide information on associated contractual language.	- Third-party security policy, standard, and procedures - Third-party risk management program - Contractual exit clauses - Related reporting and examples	GV.SC-10	EX.TR-02.01

U.S. Department
of the Treasury

TREASURY.GOV