NISTIR8477-BasedSetTheoryRelationshipMapping(STRM)
Referencedocument: Secure Controls Framework (SCF) version 2026.1
STRMGuidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **US Computer Emergency Response Team Resilience Management Model Version 1.2**
Focal Document URL: https://www.sei.cmu.edu/library/cert-resilience-management-model-cert-rmm-version-12/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-dow-cert-rmm-1-2.pdf

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
ADM:SG1	Establish Organizational Assets	Organizational assets (people, information, technology, and facilities) are identified and the authority and responsibility for these assets are established.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
ADM:SG1.SP1	Inventory Assets	Organizational assets are identified and inventoried.	Functional	Subset Of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:(1) Accurately reflects the current TAASD in use;(2) Identifies authorized software products, including business justification details;(3) Is at the level of granularity deemed necessary for tracking and reporting;(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and(5) Is available for review and audit by designated organizational personnel.	10	
ADM:SG1.SP2	Establish a Common Understanding	A common and consistent definition of assets is established and communicated.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
ADM:SG1.SP2	Establish a Common Understanding	A common and consistent definition of assets is established and communicated.	Functional	Intersects With	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	8	
ADM:SG1.SP3	Establish Ownership and Custodianship	Authority and responsibility for assets are established.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
ADM:SG1.SP3	Establish Ownership and Custodianship	Authority and responsibility for assets are established.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5	
ADM:SG1.SP3	Establish Ownership and Custodianship	Authority and responsibility for assets are established.	Functional	Intersects With	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.	5	
ADM:SG2	Establish the Relationship Between Assets and Services	The relationship between assets and the services they support is established and examined.	Functional	Subset Of	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	10	
ADM:SG2.SP1	Associate Assets with Services	Assets are associated with the service or services they support.	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5	
ADM:SG2.SP1	Associate Assets with Services	Assets are associated with the service or services they support.	Functional	Intersects With	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD).	5	
ADM:SG2.SP1	Associate Assets with Services	Assets are associated with the service or services they support.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
ADM:SG2.SP1	Associate Assets with Services	Assets are associated with the service or services they support.	Functional	Intersects With	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that:(1) Document the security categorization results (including supporting rationale) in the security plan for systems; and(2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5	
ADM:SG2.SP1	Associate Assets with Services	Assets are associated with the service or services they support.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
ADM:SG2.SP2	Analyze Asset-Service Dependencies	Instances where assets support more than one service are identified and analyzed.	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5	
ADM:SG2.SP2	Analyze Asset-Service Dependencies	Instances where assets support more than one service are identified and analyzed.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
ADM:SG3	Manage Assets	The life cycle of assets is managed.	Functional	Subset Of	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	10	
ADM:SG3.SP1	Identify Change Criteria	The criteria that would indicate changes in an asset or its association with a service are established and maintained.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
ADM:SG3.SP1	Identify Change Criteria	The criteria that would indicate changes in an asset or its association with a service are established and maintained.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
ADM:SG3.SP2	Maintain Changes to Assets and Inventory	Changes to assets are managed as conditions dictate.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
ADM:SG3.SP2	Maintain Changes to Assets and Inventory	Changes to assets are managed as conditions dictate.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
ADM:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Asset Definition and Management process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
ADM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Asset Definition and Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
ADM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Asset Definition and Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
ADM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Asset Definition and Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
ADM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Asset Definition and Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
ADM:GG2	Institutionalize a Managed Process	Asset definition and management is institutionalized as a managed process.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
ADM:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the asset definition and management process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
ADM:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the asset definition and management process.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
ADM:GG2.GP3	Provide Resources	Provide adequate resources for performing the asset definition and management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
ADM:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the asset definition and management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
ADM:GG2.GP5	Train People	Train the people performing or supporting the asset definition and management process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
ADM:GG2.GP6	Control Work Products	Place designated work products of the asset definition and management process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
ADM:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the asset definition and management process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
ADM:GG2.GP8	Measure and Control the Process	Measure and control the asset definition and management process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
ADM:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the asset definition and management process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
ADM:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the asset definition and management process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
ADM:GG3	Institutionalize a Defined Process	Asset definition and management is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
ADM:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined asset definition and management process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
ADM:GG3.GP2	Collect Improvement Information	Collect asset definition and management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
AM:SG1	Manage and Control Access	Access granted to organizational assets is managed and controlled.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
AM:SG1.SP1	Enable Access	Appropriate access to organizational assets is established based on resilience requirements and appropriate approvals.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
AM:SG1.SP2	Manage Changes to Access Privileges	Changes to access privileges are managed as assets, roles, and resilience requirements change.	Functional	Intersects With	System Account Reviews	IAC-15.7	Mechanisms exist to review all system accounts and disable any account that cannot be associated with a business process and owner.	5	
AM:SG1.SP3	Periodically Review and Maintain Access Privileges	Periodic review is performed to identify excessive or inappropriate levels of access privileges.	Functional	Intersects With	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	
AM:SG1.SP4	Correct Inconsistencies	Excessive or inappropriate levels of access privileges are corrected.	Functional	Intersects With	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
AM:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Access Management process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
AM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Access Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
AM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Access Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
AM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Access Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
AM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Access Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
AM:GG2	Institutionalize a Managed Process	Access management is institutionalized as a managed process.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
AM:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the access management process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
AM:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the access management process.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
AM:GG2.GP3	Provide Resources	Provide adequate resources for performing the access management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
AM:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the access management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
AM:GG2.GP5	Train People	Train the people performing or supporting the access management process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
AM:GG2.GP6	Control Work Products	Place designated work products of the access management process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
AM:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the access management process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
AM:GG2.GP8	Measure and Control the Process	Measure and control the access management process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
AM:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the access management process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
AM:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the access management process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
AM:GG3	Institutionalize a Defined Process	Access management is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
AM:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined access management process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
AM:GG3.GP2	Collect Improvement Information	Collect access management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
COMM:SG1	Prepare for Resilience Communications	A plan for developing, deploying, and managing resilience communications is established and maintained.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
COMM:SG1.SP1	Establish a Resilience Communications Plan	Planning for the resilience communications process is performed.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
COMM:SG1.SP2	Identify Communications Requirements	The types and extent of communications needed by the organization to support stakeholder and organizational information needs are identified.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
COMM:SG1.SP3	Establish Communications Guidelines and Standards	The guidelines and standards for satisfying communications needs are established and maintained.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
COMM:SG2	Deliver Resilience Communications	The activities necessary to deliver communications for resilience activities on an operational and event-driven basis are established and maintained.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
COMM:SG2.SP1	Identify Communications Methods and Channels	Communications methods and channels relevant to stakeholder and organizational needs are established and maintained.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
COMM:SG2.SP2	Establish and Maintain Communications Infrastructure	An infrastructure appropriate to meet the organization's resilience communications needs is established and maintained.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
COMM:SG2.SP3	Provide Resilience Communications	Resilience communications are delivered according to the communications plan.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
COMM:SG3	Improve Communications	Resilience communications are reviewed to identify and implement improvements in the communications process.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
COMM:SG3.SP1	Assess Communications Effectiveness	The effectiveness of resilience communications plans and programs is assessed and corrective actions are identified.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
COMM:SG3.SP2	Improve Communications	Lessons learned in managing resilience communications are used to improve communications plans.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
COMM:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Communications process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
COMM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Communications process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
COMM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Communications process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
COMM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Communications process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
COMM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Communications process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
COMM:GG2	Institutionalize a Managed Process	Communications is institutionalized as a managed process.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
COMM:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the communications process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
COMM:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the communications process.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
COMM:GG2.GP3	Provide Resources	Provide adequate resources for performing the communications process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
COMM:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the communications process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
COMM:GG2.GP5	Train People	Train the people performing or supporting the communications process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
COMM:GG2.GP6	Control Work Products	Place designated work products of the communications process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
COMM:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the communications process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
COMM:GG2.GP8	Measure and Control the Process	Measure and control the communications process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
COMM:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the communications process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
COMM:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the communications process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
COMM:GG3	Institutionalize a Defined Process	Communications is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
COMM:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined communications process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
COMM:GG3.GP2	Collect Improvement Information	Collect communications work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
COMP:SG1	Prepare for Compliance Management	The organizational environment and processes for identifying, satisfying, and monitoring compliance obligations are established.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
COMP:SG1.SP1	Establish a Compliance Plan	A strategic plan for managing compliance to obligations is established.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
COMP:SG1.SP2	Establish a Compliance Program	A program is established to carry out the activities and practices of the compliance plan.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
COMP:SG1.SP3	Establish Compliance Guidelines and Standards	The guidelines and standards for satisfying compliance obligations are established and communicated.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
COMP:SG2	Establish Compliance Obligations	The organization's compliance obligations are identified, documented, and communicated.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
COMP:SG2.SP1	Identify Compliance Obligations	Compliance obligations are identified and documented.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
COMP:SG2.SP2	Analyze Obligations	Compliance obligations are analyzed and organized to facilitate satisfaction.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
COMP:SG2.SP3	Establish Ownership for Meeting Obligations	The responsibility for satisfying compliance obligations is established.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
COMP:SG3	Demonstrate Satisfaction of Compliance Obligations	The organization demonstrates that its compliance obligations are being satisfied.	Functional	Intersects With	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document:(1) Is concise;(2) Unambiguously reflects the current status;(3) Is physically or electronically signed; and(4) Where possible, is machine readable.	5	
COMP:SG3.SP1	Collect and Validate Compliance Data	Data required to satisfy compliance obligations is collected and validated.	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-01.3	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5	
COMP:SG3.SP2	Demonstrate the Extent of Compliance Obligation Satisfaction	The extent to which compliance obligations are satisfied is demonstrated through compliance activities.	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-01.3	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5	
COMP:SG3.SP3	Remediate Areas of Non-Compliance	Remediation of areas of non-compliance is performed to ensure satisfaction of compliance obligations.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
COMP:SG4	Monitor Compliance Activities	The organization's satisfaction of compliance obligations is monitored and adjusted as necessary.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
COMP:SG4.SP1	Evaluate Compliance Activities	Satisfaction of the organization's compliance obligations is independently monitored and improved.	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	5	
COMP:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Compliance process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
COMP:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Compliance process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
COMP:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Compliance process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
COMP:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Compliance process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
COMP:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Compliance process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
COMP:GG2	Institutionalize a Managed Process	Compliance is institutionalized as a managed process.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
COMP:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the compliance process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
COMP:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the compliance process.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
COMP:GG2.GP3	Provide Resources	Provide adequate resources for performing the compliance process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
COMP:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the compliance process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
COMP:GG2.GP5	Train People	Train the people performing or supporting the compliance process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
COMP:GG2.GP6	Control Work Products	Place designated work products of the compliance process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
COMP:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the compliance process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
COMP:GG2.GP8	Measure and Control the Process	Measure and control the compliance process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
COMP:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the compliance process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
COMP:GG2.GP10	Review Status with Higher level Managers	Review the activities, status, and results of the compliance process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
COMP:GG3	Institutionalize a Defined Process	Compliance is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
COMP:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined compliance process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
COMP:GG3.GP2	Collect Improvement Information	Collect compliance work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
CTRL:SG1	Establish Control Objectives	Organizational objectives to be achieved through the selection and implementation of controls are established.	Functional	Intersects With	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal security, compliance and resilience control system.	5	
CTRL:SG1.SP1	Define Control Objectives	Control objectives are established as the basis for the selection, implementation, and management of the organization's internal control system.	Functional	Intersects With	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal security, compliance and resilience control system.	5	
CTRL:SG2	Establish Controls	Controls that support control objectives and strategies for protecting and sustaining high-value services and assets are established.	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
CTRL:SG2.SP1	Define Controls	Controls that protect services and assets from disruption are identified and established.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
CTRL:SG3	Analyze Controls	Controls are analyzed to ensure they satisfy control objectives.	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are:(1) Implemented correctly; and(2) Operating as intended.	5	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CTRL:SG3.SP1	Analyze Controls	Controls are analyzed to determine their ability to achieve control objectives.	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are:(1) Implemented correctly; and(2) Operating as intended.	5	
CTRL:SG4	Assess Control Effectiveness	The ability of the internal control system to satisfy resilience requirements is assessed.	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are:(1) Implemented correctly; and(2) Operating as intended.	5	
CTRL:SG4.SP1	Assess Controls	Controls are assessed for effectiveness in meeting control objectives and satisfying resilience requirements.	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are:(1) Implemented correctly; and(2) Operating as intended.	5	
CTRL:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Controls Management process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
CTRL:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Controls Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
CTRL:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Controls Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
CTRL:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Controls Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
CTRL:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Controls Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
CTRL:GG2	Institutionalize a Managed Process	Controls management is institutionalized as a managed process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
CTRL:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the controls management process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
CTRL:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the controls management process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
CTRL:GG2.GP3	Provide Resources	Provide adequate resources for performing the controls management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
CTRL:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the controls management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
CTRL:GG2.GP5	Train People	Train the people performing or supporting the controls management process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
CTRL:GG2.GP6	Control Work Products	Place designated work products of the controls management process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
CTRL:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the controls management process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
CTRL:GG2.GP8	Measure and Control the Process	Measure and control the controls management process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
CTRL:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the controls management process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
CTRL:GG2.GP10	Review Status with Higher level Managers	Review the activities, status, and results of the controls management process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
CTRL:GG3	Institutionalize a Defined Process	Controls management is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
CTRL:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined controls management process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
CTRL:GG3.GP2	Collect Improvement Information	Collect controls management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
EC:SG1	Establish and Prioritize Facility Assets	Facility assets are prioritized to ensure resilience of high-value services that they support.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
EC:SG1.SP1	Prioritize Facility Assets	Facility assets are prioritized relative to their importance in supporting the delivery of high-value services.	Functional	Subset Of	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	10	
EC:SG1.SP2	Establish Resilience-Focused Facility Assets	Facility assets that specifically support the organization's service continuity plans are identified and established.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
EC:SG2	Protect Facility Assets	Administrative, technical, and physical controls for facility assets are identified, implemented, monitored, and managed.	Functional	Subset Of	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
EC:SG2.SP1	Assign Resilience Requirements to Facility Assets	Resilience requirements that have been defined are assigned to facility assets.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
EC:SG2.SP2	Establish and Implement Controls	Administrative, technical, and physical controls that are required to meet the established resilience requirements are identified and implemented.	Functional	Subset Of	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
EC:SG3	Manage Facility Asset Risk	Operational and environmental risks to facility assets are identified and managed.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
EC:SG3.SP1	Identify and Assess Facility Asset Risks	Risks to facility assets are periodically identified and assessed.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
EC:SG3.SP2	Address Facility Risks	Risk response plans for risks to facility assets are developed and implemented.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	
EC:SG4	Control Operational Environment	The operational environment of the facility is controlled to ensure its availability.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
EC:SG4.SP1	Perform Facility Sustainability Planning	The availability of high-value facilities is ensured through sustainability planning.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
EC:SG4.SP1	Perform Facility Sustainability Planning	The availability of high-value facilities is ensured through sustainability planning.	Functional	Intersects With	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5	
EC:SG4.SP2	Maintain Environmental Conditions	Environmental conditions of facility assets are maintained.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
EC:SG4.SP3	Manage Dependencies on Public Services	Dependencies on public services for facility assets are identified and managed.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
EC:SG4.SP4	Manage Dependencies on Public Infrastructure	Dependencies on public infrastructure for facility assets are identified and managed.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
EC:SG4.SP5	Plan for Facility Retirement	Facility retirements are planned in order to minimize operational impact.	Functional	Intersects With	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	5	
EC:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Environmental Control process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
EC:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Environmental Control process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
EC:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Environmental Control process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
EC:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Environmental Control process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
EC:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Environmental Control process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
EC:GG2	Institutionalize a Managed Process	Environmental control is institutionalized as a managed process.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
EC:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the environmental control process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
EC:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the environmental control process.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
EC:GG2.GP3	Provide Resources	Provide adequate resources for performing the environmental control process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
EC:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the environmental control process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
EC:GG2.GP5	Train People	Train the people performing or supporting the environmental control process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
EC:GG2.GP6	Control Work Products	Place designated work products of the environmental control process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
EC:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the environmental control process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
EC:GG2.GP8	Measure and Control the Process	Measure and control the environmental control process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
EC:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the environmental control process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
EC:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the environmental control process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
EC:GG3	Institutionalize a Defined Process	Environmental control is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
EC:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined environmental control process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
EC:GG3.GP2	Collect Improvement Information	Collect environmental control work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
EF:SG1	Establish Strategic Objectives	The strategic objectives of the organization are established as the foundation for the operational resilience management system.	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a:(1) Strategic security, compliance and resilience-specific business plan; and(2) Set of objectives to achieve that plan.	5	
EF:SG1.SP1	Establish Strategic Objectives	Strategic objectives are identified and established as the basis for resilience activities.	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a:(1) Strategic security, compliance and resilience-specific business plan; and(2) Set of objectives to achieve that plan.	5	
EF:SG1.SP2	Establish Critical Success Factors	The critical success factors of the organization are identified and established.	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a:(1) Strategic security, compliance and resilience-specific business plan; and(2) Set of objectives to achieve that plan.	5	
EF:SG1.SP3	Establish Organizational Services	The high-value services that support the accomplishment of strategic objectives are established.	Functional	Intersects With	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	5	
EF:SG2	Plan for Operational Resilience	Planning for the operational resilience management system is performed.	Functional	Intersects With	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	5	
EF:SG2.SP1	Establish an Operational Resilience Management Plan	A plan for managing operational resilience is established as the basis for the operational resilience management program.	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a:(1) Strategic security, compliance and resilience-specific business plan; and(2) Set of objectives to achieve that plan.	5	
EF:SG2.SP2	Establish an Operational Resilience Management Program	A program is established to carry out the activities and practices of the operational resilience management plan.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
EF:SG3	Establish Sponsorship	Visible sponsorship of higher level managers for the operational resilience management system is established.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
EF:SG3.SP1	Commit Funding for Operational Resilience Management	A commitment by higher level managers to fund resilience activities is established.	Functional	Intersects With	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including:(1) Staffing;(2) Budget;(3) Processes; and(4) Technologies.	5	
EF:SG3.SP2	Promote a Resilience-Aware Culture	A resilience-aware culture is promoted through goal setting and achievement.	Functional	Intersects With	Business As Usual (BAU) Security, Compliance & Resilience Practices	GOV-14	Mechanisms exist to incorporate security, compliance and resilience principles into Business As Usual (BAU) practices through executive leadership involvement.	5	
EF:SG3.SP3	Sponsor Resilience Standards and Policies	The development, implementation, enforcement, and management of resilience standards and policies are sponsored.	Functional	Intersects With	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including:(1) Staffing;(2) Budget;(3) Processes; and(4) Technologies.	5	
EF:SG4	Provide Resilience Oversight	Governance over the operational resilience management system is established and performed.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
EF:SG4.SP1	Establish Resilience as a Governance Focus Area	Governance activities are extended to the operational resilience management system and accomplishment of the process goals.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
EF:SG4.SP2	Perform Resilience Oversight	Oversight is performed over the operational resilience management system for adherence to established procedures, policies, standards, guidelines, and regulations.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
EF:SG4.SP3	Establish Corrective Actions	Corrective actions are identified to address performance issues.	Functional	Intersects With	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including:(1) Staffing;(2) Budget;(3) Processes; and(4) Technologies.	5	
EF:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Enterprise Focus process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
EF:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Enterprise Focus process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
EF:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Enterprise Focus process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	10	
EF:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Enterprise Focus process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
EF:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Enterprise Focus process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
EF:GG2	Institutionalize a Managed Process	Enterprise focus is institutionalized as a managed process.	Functional	Subset Of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	10	
EF:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the enterprise focus process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
EF:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the enterprise focus process.	Functional	Subset Of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	10	
EF:GG2.GP3	Provide Resources	Provide adequate resources for performing the enterprise focus process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
EF:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the enterprise focus process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
EF:GG2.GP5	Train People	Train the people performing or supporting the enterprise focus process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
EF:GG2.GP6	Control Work Products	Place designated work products of the enterprise focus process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
EF:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the enterprise focus process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
EF:GG2.GP8	Measure and Control the Process	Measure and control the enterprise focus process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
EF:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the enterprise focus process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
EF:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the enterprise focus process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
EF:GG3	Institutionalize a Defined Process	Enterprise focus is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
EF:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined enterprise focus process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
EF:GG3.GP2	Collect Improvement Information	Collect enterprise focus work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
EXD:SG1	Identify and Prioritize External Dependencies	External dependencies are identified and prioritized to ensure the resilience of the high-value services that they support	Functional	Intersects With	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
EXD:SG1.SP1	Identify External Dependencies	A list of external dependencies is established and maintained.	Functional	Intersects With	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
EXD:SG1.SP2	Prioritize External Dependencies	External dependencies are prioritized relative to their importance in supporting the delivery of high-value services.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
EXD:SG2	Manage Risks Due to External Dependencies	Risks due to external dependencies are identified and managed.	Functional	Subset Of	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to:(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	10	
EXD:SG2.SP1	Identify and Assess Risks Due to External Dependencies	Risks associated with external dependencies are periodically identified and assessed.	Functional	Subset Of	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to:(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	10	
EXD:SG2.SP2	Mitigate Risks Due to External Dependencies	Risk mitigation plans for risks to due external dependencies are developed and implemented.	Functional	Subset Of	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to:(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	10	
EXD:SG3	Establish Formal Relationships	Relationships with external entities are formally established and maintained.	Functional	Subset Of	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to:(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	10	
EXD:SG3.SP1	Establish Enterprise Specifications for External Dependencies	Enterprise specifications that apply in general to external entities are established and maintained.	Functional	Subset Of	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to:(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	10	
EXD:SG3.SP2	Establish Resilience Specifications for External Dependencies	Resilience specifications that apply to specific external dependencies and entities are established and maintained	Functional	Subset Of	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to:(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	10	
EXD:SG3.SP3	Evaluate and Select External Entities	External entities are selected based on an evaluation of their ability to meet the specifications for external dependencies.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
EXD:SG3.SP4	Formalize Relationships	Formal agreements with external entities are established and maintained.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
EXD:SG4	Manage External Entity Performance	The performance of external entities is managed.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	
EXD:SG4.SP1	Monitor External Entity Performance	The performance of external entities is monitored against the specifications.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	
EXD:SG4.SP2	Correct External Entity Performance	Corrective actions are implemented to support external entity performance as necessary.	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
EXD:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the External Dependencies Management process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
EXD:GG1.GP1	Perform Specific Practices	Perform the specific practices of the External Dependencies Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
EXD:GG1.GP1	Perform Specific Practices	Perform the specific practices of the External Dependencies Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
EXD:GG1.GP1	Perform Specific Practices	Perform the specific practices of the External Dependencies Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
EXD:GG1.GP1	Perform Specific Practices	Perform the specific practices of the External Dependencies Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
EXD:GG2	Institutionalize a Managed Process	External dependencies management is institutionalized as a managed process.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
EXD:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the external dependencies management process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
EXD:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the external dependencies management process.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
EXD:GG2.GP3	Provide Resources	Provide adequate resources for performing the external dependencies management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
EXD:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the external dependencies management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
EXD:GG2.GP5	Train People	Train the people performing or supporting the external dependencies management process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
EXD:GG2.GP6	Control Work Products	Place designated work products of the external dependencies management process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
EXD:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the external dependencies management process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
EXD:GG2.GP8	Measure and Control the Process	Measure and control the external dependencies management process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
EXD:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the external dependencies management process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
EXD:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the external dependencies management process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
EXD:GG3	Institutionalize a Defined Process	External dependencies management is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
EXD:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined external dependencies management process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
EXD:GG3.GP2	Collect Improvement Information	Collect external dependencies work products, measures, measurement results, and improvement information derived from planning and performing the process to support the future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
FRM:SG1	Establish Financial Commitment	A commitment to funding resilience activities is established.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:SG1.SP1	Commit Funding for Operational Resilience Management	A commitment by higher level managers to fund resilience activities is established.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:SG1.SP2	Establish Structure to Support Financial Management	The structure that supports the assignment and management of financial resources to resilience activities is established.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:SG2	Perform Financial Planning	Planning for funding resilience management activities is performed.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:SG2.SP1	Define Funding Needs	The financial obligations for managing the operational resilience management system are established.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:SG2.SP2	Establish Resilience Budgets	Capital and expense budgets for resilience management are established.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:SG2.SP3	Resolve Funding Gaps	Identify and resolve gaps in funding for resilience management and address associated risks.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
FRM:SG3	Fund Resilience Activities	The organization's essential activities for managing and sustaining operational resilience are funded.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:SG3.SP1	Fund Resilience Activities	Access to funds for resilience management activities is provided.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:SG4	Account for Resilience Activities	Accounting for the financial commitment to resilience activities is performed and used for process improvement.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:SG4.SP1	Track and Document Costs	The costs associated with resilience management are tracked and documented.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:SG4.SP2	Perform Cost and Performance Analysis	Cost and performance analysis for funded resilience management activities is performed.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:SG5	Optimize Resilience Expenditures and Investments	The return to the organization for investment in resilience activities is measured and assessed.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:SG5.SP1	Optimize Resilience Expenditures	The costs to implement and manage strategies to protect and sustain services and assets are optimized against the benefits.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:SG5.SP2	Determine Return on Resilience Investments	A return on resilience investments is calculated where possible.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:SG5.SP3	Identify Cost Recovery Opportunities	Opportunities for the organization to recover costs and investments in resilience management activities are identified.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Financial Resource Management process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
FRM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Financial Resource Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
FRM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Financial Resource Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Financial Resource Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
FRM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Financial Resource Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
FRM:GG2	Institutionalize a Managed Process	Financial resource management is institutionalized as a managed process.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the financial resource management process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
FRM:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the financial resource management process.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
FRM:GG2.GP3	Provide Resources	Provide adequate resources for performing the financial resource management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
FRM:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the financial resource management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
FRM:GG2.GP5	Train People	Train the people performing or supporting the financial resource management process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
FRM:GG2.GP6	Control Work Products	Place designated work products of the financial resource management process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
FRM:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the financial resource management process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
FRM:GG2.GP8	Measure and Control the Process	Measure and control the financial resource management process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
FRM:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the financial resource management process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
FRM:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the financial resource management process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
FRM:GG3	Institutionalize a Defined Process	Financial resource management is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
FRM:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined financial resource management process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
FRM:GG3.GP2	Collect Improvement Information	Collect financial resource management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
HRM:SG1	Establish Resource Needs	The resource needs to staff the activities and tasks of the organization's resilience program and plan are identified and satisfied.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HRM:SG1.SP1	Establish Baseline Competencies	The staffing and skill needs relative to the operational resilience management system are established.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HRM:SG1.SP2	Inventory Skills and Identify Gaps	The current skill set for operational resilience management is inventoried and gaps in necessary skills are identified.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HRM:SG1.SP3	Address Skill Deficiencies	Gaps in skills necessary to meet operational resilience management needs are addressed.	Functional	Intersects With	Identify Critical Skills & Gaps	HRS-13	Mechanisms exist to evaluate the critical security, compliance and resilience skills needed to support the organization's mission and identify gaps that exist.	5	
HRM:SG2	Manage Staff Acquisition	The acquisition of staff to meet operational needs is performed with consideration of the organization's resilience objectives.	Functional	Intersects With	Remediate Identified Skills Deficiencies	HRS-13.1	Mechanisms exist to remediate critical skills deficiencies necessary to support the organization's mission and business functions.	5	
HRM:SG2.SP1	Verify Suitability of Candidate Staff	Candidate staff are evaluated for suitability against position requirements and risks.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HRM:SG2.SP2	Establish Terms and Conditions of Employment	Employment agreements appropriate for the position and role are developed and executed.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HRM:SG3	Manage Staff Performance	The performance of staff to support the organization's resilience program is managed.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HRM:SG3.SP1	Establish Resilience as a Job Responsibility	Resilience obligations for staff are communicated, agreed to, and documented as conditions of employment.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
HRM:SG3.SP2	Establish Resilience Performance Goals and Objectives	Goals and objectives for supporting the organization's resilience program are established as part of the performance management process.	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	
HRM:SG3.SP3	Measure and Assess Performance	Performance against goals and objectives is measured, achievements are acknowledged, and corrective actions are identified and communicated.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HRM:SG3.SP4	Establish Disciplinary Process	A disciplinary process is established for staff who violate resilience policies.	Functional	Subset Of	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	10	
HRM:SG4	Manage Changes to Employment Status	Changes in the employment status of staff members in the organization are managed.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HRM:SG4.SP1	Manage Impact of Position Changes	Administrative controls are established to sustain functions, obligations, and vital roles upon position changes or terminations.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HRM:SG4.SP2	Manage Access to Assets	Access to and possession of organizational assets relative to position changes is managed.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HRM:SG4.SP3	Manage Involuntary Terminations	Administrative controls and procedures are established to manage the effects of involuntary terminations.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HRM:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Human Resource Management process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
HRM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Human Resource Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
HRM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Human Resource Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HRM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Human Resource Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
HRM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Human Resource Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
HRM:GG2	Institutionalize a Managed Process	Human resource management is institutionalized as a managed process.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HRM:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the human resource management process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
HRM:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the human resource management process.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HRM:GG2.GP3	Provide Resources	Provide adequate resources for performing the human resource management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
HRM:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the human resource management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
HRM:GG2.GP5	Train People	Train the people performing or supporting the human resource management process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
HRM:GG2.GP6	Control Work Products	Place designated work products of the human resource management process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
HRM:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the human resource management process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
HRM:GG2.GP8	Measure and Control the Process	Measure and control the human resource management process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
HRM:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the human resource management process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
HRM:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the human resource management process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
HRM:GG3	Institutionalize a Defined Process	Human resource management is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
HRM:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined human resource management process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
HRM:GG3.GP2	Collect Improvement Information	Collect human resource management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
ID:SG1	Establish Identities	Identities are created to represent persons, objects, and entities that require access to organizational assets.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ID:SG1.SP1	Create Identities	Persons, objects, and entities that require access to organizational assets are registered and profiled.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ID:SG1.SP2	Establish Identity Community	The identity community is established and documented.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ID:SG1.SP3	Assign Roles to Identities	Organizational roles are established and associated with identities.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ID:SG2	Manage Identities	Identities are managed to ensure they reflect the current environment of associated persons, objects, and entities.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ID:SG2.SP1	Monitor and Manage Identity Changes	Changes to identities are monitored for and managed.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ID:SG2.SP2	Periodically Review and Maintain Identities	Periodic review is performed to identify identities that are invalid.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ID:SG2.SP3	Correct Inconsistencies	Inconsistencies between the identity community and the persons, objects, and entities they represent are corrected.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ID:SG2.SP4	Deprovision Identities	Identities for which need has expired or has been eliminated are deprovisioned.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ID:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Identity Management process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
ID:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Identity Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
ID:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Identity Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ID:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Identity Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
ID:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Identity Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
ID:GG2	Institutionalize a Managed Process	Identity management is institutionalized as a managed process.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ID:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the identity management process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
ID:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the identity management process.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ID:GG2.GP3	Provide Resources	Provide adequate resources for performing the identity management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
ID:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the identity management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
ID:GG2.GP5	Train People	Train the people performing or supporting the identity management process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
ID:GG2.GP6	Control Work Products	Place designated work products of the identity management process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
ID:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the identity management process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
ID:GG2.GP8	Measure and Control the Process	Measure and control the identity management process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
ID:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the identity management process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
ID:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the identity management process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
ID:GG3	Institutionalize a Defined Process	Identity management is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
ID:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined identity management process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
ID:GG3.GP2	Collect Improvement Information	Collect identity management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
IMC:SG1	Establish the Incident Management and Control Process	The organizational process for identifying, analyzing, responding to, and learning from incidents is established.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
IMC:SG1.SP1	Plan for Incident Management	Planning is performed for developing and implementing the organization's incident management and control process.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
IMC:SG1.SP2	Assign Staff to the Incident Management Plan	Staff are identified and assigned to the incident management plan.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
IMC:SG2	Detect Events	A process for detecting, reporting, triaging, and analyzing events is established and maintained.	Functional	Subset Of	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	10	
IMC:SG2.SP1	Detect and Report Events	Events are detected and reported.	Functional	Subset Of	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	10	
IMC:SG2.SP2	Log and Track Events	Events are logged and tracked from inception to disposition.	Functional	Subset Of	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	10	
IMC:SG2.SP3	Collect, Document, and Preserve Event Evidence	The process for collecting, documenting, and preserving event evidence is established and managed.	Functional	Subset Of	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	10	
IMC:SG2.SP4	Analyze and Triage Events	Events are analyzed and triaged to support event resolution and incident declaration.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
IMC:SG3	Declare and Analyze Incidents	Incidents are declared and analyzed to support response planning.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
IMC:SG3.SP1	Declare Incidents	Incidents are declared based on criteria that are established and maintained.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
IMC:SG3.SP2	Analyze Incidents	Incidents are analyzed to support the development of an appropriate incident response.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IMC:SG4	Respond to and Recover from Incidents	The process for responding to and recovering from incidents is established.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
IMC:SG4.SP1	Escalate Incidents	Incidents are escalated to the appropriate stakeholders for input and resolution.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
IMC:SG4.SP2	Develop Incident Response	A response to a declared incident is developed and implemented to prevent or limit organizational impact.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
IMC:SG4.SP3	Communicate Incidents	A plan for the communication of incidents to relevant stakeholders and a process for managing ongoing incident communications are established.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
IMC:SG4.SP4	Close Incidents	Incidents are closed after relevant actions have been taken by the organization.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
IMC:SG5	Establish Incident Learning	Lessons learned from identifying, analyzing, and responding to incidents are translated into actions to improve strategies for protecting and sustaining services and assets.	Functional	Subset Of	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	10	
IMC:SG5.SP1	Perform Post-Incident Review	Post-incident review is performed to determine underlying causes.	Functional	Subset Of	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	10	
IMC:SG5.SP2	Translate Experience to Strategy	The lessons learned from incident management are analyzed and translated into improvements.	Functional	Subset Of	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	10	
IMC:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Incident Management and Control process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
IMC:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Incident Management and Control process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
IMC:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Incident Management and Control process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
IMC:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Incident Management and Control process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
IMC:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Incident Management and Control process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
IMC:GG2	Institutionalize a Managed Process	Incident management and control is institutionalized as a managed process.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
IMC:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the incident management and control process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
IMC:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the incident management and control process.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
IMC:GG2.GP3	Provide Resources	Provide adequate resources for performing the incident management and control process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
IMC:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the incident management and control process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
IMC:GG2.GP5	Train People	Train the people performing or supporting the incident management and control process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
IMC:GG2.GP6	Control Work Products	Place designated work products of the incident management and control process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
IMC:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the incident management and control process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
IMC:GG2.GP8	Measure and Control the Process	Measure and control the incident management and control process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
IMC:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the incident management and control process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
IMC:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the incident management and control process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
IMC:GG3	Institutionalize a Defined Process	Incident management and control is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
IMC:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined incident management and control process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
IMC:GG3.GP2	Collect Improvement Information	Collect incident management and control work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
KIM:SG1	Establish and Prioritize Information Assets	Information assets are prioritized to ensure the resilience of high-value services in which they are used.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
KIM:SG1.SP1	Prioritize Information Assets	Information assets are prioritized relative to their importance in supporting the delivery of high-value services.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
KIM:SG1.SP2	Categorize Information Assets	Information assets that support high-value services are categorized as to their organizational sensitivity.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
KIM:SG2	Protect Information Assets	Administrative, technical, and physical controls for information assets are identified, implemented, monitored, and managed.	Functional	Subset Of	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
KIM:SG2.SP1	Assign Resilience Requirements to Information Assets	Resilience requirements that have been defined are assigned to information assets.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
KIM:SG2.SP2	Establish and Implement Controls	Administrative, technical, and physical controls that are required to meet the established resilience requirements are identified and implemented.	Functional	Subset Of	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
KIM:SG3	Manage Information Asset Risks	Operational risks to information assets are identified and managed.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
KIM:SG3.SP1	Identify and Assess Information Asset Risks	Risks to information assets are periodically identified and assessed.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
KIM:SG3.SP2	Address Information Asset Risks	Risk response plans for risks to information assets are developed and implemented.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	
KIM:SG4	Manage Information Asset Confidentiality and Privacy	The confidentiality and privacy considerations of information assets are managed.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
KIM:SG4.SP1	Encrypt High-Value Information	Cryptographic controls are applied to information assets to ensure confidentiality and prevent accidental disclosure.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
KIM:SG4.SP2	Control Access to Information Assets	Access controls are developed and implemented to limit access to information assets.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
KIM:SG4.SP3	Control Information Asset Disposition	The means for disposing of information assets are controlled.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
KIM:SG5	Manage Information Asset Integrity	The integrity of information assets to support high-value services is managed.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
KIM:SG5.SP1	Control Modification of Information Assets	The modification of information assets is controlled.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
KIM:SG5.SP2	Manage Information Asset Configuration	Information asset baselines are created and changes are managed.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
KIM:SG5.SP3	Verify Validity of Information	Controls are implemented to sustain the validity and reliability of information assets	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
KIM:SG6	Manage Information Asset Availability	The availability of information assets to support high-value services is managed.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
KIM:SG6.SP1	Perform Information Duplication and Retention	High-value information assets are backed up and retained to support services when needed.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
KIM:SG6.SP2	Manage Organizational Knowledge	The organizational and intellectual knowledge of staff is identified and documented.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
KIM:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Knowledge and Information Management process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
KIM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Knowledge and Information Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
KIM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Knowledge and Information Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
KIM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Knowledge and Information Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
KIM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Knowledge and Information Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
KIM:GG2	Institutionalize a Managed Process	Knowledge and information management is institutionalized as a managed process.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
KIM:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the knowledge and information management process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
KIM:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the knowledge and information management process.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
KIM:GG2.GP3	Provide Resources	Provide adequate resources for performing the knowledge and information management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
KIM:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the knowledge and information management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
KIM:GG2.GP5	Train People	Train the people performing or supporting the knowledge and information management process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
KIM:GG2.GP6	Control Work Products	Place designated work products of the knowledge and information management process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
KIM:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the knowledge and information management process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
KIM:GG2.GP8	Measure and Control the Process	Measure and control the knowledge and information management process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
KIM:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the knowledge and information management process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
KIM:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the knowledge and information management process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
KIM:GG3	Institutionalize a Defined Process	Knowledge and information management is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
KIM:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined knowledge and information management process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
KIM:GG3.GP2	Collect Improvement Information	Collect knowledge and information management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
MA:SG1	Align Measurement and Analysis Activities	Measurement objectives and activities are aligned with identified information needs and objectives.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
MA:SG1.SP1	Establish Measurement Objectives	Measurement objectives are established and maintained based on information needs and objectives.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
MA:SG1.SP2	Specify Measures	The measures necessary to meet measurement objectives are established.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
MA:SG1.SP3	Specify Data Collection and Storage Procedures	The techniques for collecting and storing measurement data are specified.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
MA:SG1.SP4	Specify Analysis Procedures	The techniques for analysis and reporting are specified.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
MA:SG2	Provide Measurement Results	Measurement results, which address identified information needs and objectives, are provided.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
MA:SG2.SP1	Collect Measurement Data	Measurement data is collected consistent with measurement objectives.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
MA:SG2.SP2	Analyze Measurement Data	Measurement data is analyzed against measurement objectives.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
MA:SG2.SP3	Store Data and Results	Measurement data, analyses, and results are stored.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
MA:SG2.SP4	Communicate Results	The results of measurement and analysis activities are communicated to relevant stakeholders.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
MA:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Measurement and Analysis process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
MA:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Measurement and Analysis process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
MA:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Measurement and Analysis process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
MA:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Measurement and Analysis process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
MA:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Measurement and Analysis process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
MA:GG2	Institutionalize a Managed Process	Measurement and analysis is institutionalized as a managed process.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
MA:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the measurement and analysis process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
MA:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the measurement and analysis process.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
MA:GG2.GP3	Provide Resources	Provide adequate resources for performing the measurement and analysis process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
MA:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the measurement and analysis process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
MA:GG2.GP5	Train People	Train the people performing or supporting the measurement and analysis process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
MA:GG2.GP6	Control Work Products	Place designated work products of the measurement and analysis process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
MA:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the measurement and analysis process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
MA:GG2.GP8	Measure and Control the Process	Measure and control the measurement and analysis process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
MA:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the measurement and analysis process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
MA:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the measurement and analysis process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
MA:GG3	Institutionalize a Defined Process	Measurement and analysis is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
MA:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined measurement and analysis process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
MA:GG3.GP2	Collect Improvement Information	Collect measurement and analysis work products and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
MON:SG1	Establish and Maintain a Monitoring Program	A program for identifying, recording, collecting, and reporting important resilience information is established and maintained.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON:SG1.SP1	Establish a Monitoring Program	A program for identifying, collecting, and distributing monitoring information is established and maintained.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON:SG1.SP2	Identify Stakeholders	The organizational and external entities that rely upon information collected from the monitoring process are identified.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
MON:SG1.SP3	Establish Monitoring Requirements	The requirements for monitoring operational resilience management processes are established.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON:SG1.SP4	Analyze and Prioritize Monitoring Requirements	Monitoring requirements are analyzed and prioritized to ensure they can be satisfied.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON:SG2	Perform Monitoring	The monitoring process is performed throughout the enterprise.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON:SG2.SP1	Establish and Maintain Monitoring Infrastructure	A monitoring infrastructure commensurate with meeting monitoring requirements is established and maintained.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON:SG2.SP2	Establish Collection Standards and Guidelines	The standards and parameters for collecting information and managing data are established.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON:SG2.SP3	Collect and Record Information	Information relevant to the operational resilience management system is collected and recorded.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON:SG2.SP4	Distribute Information	Collected and recorded information is distributed to appropriate stakeholders.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Monitoring process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
MON:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Monitoring process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
MON:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Monitoring process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Monitoring process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
MON:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Monitoring process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
MON:GG2	Institutionalize a Managed Process	Monitoring is institutionalized as a managed process.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the monitoring process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
MON:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the monitoring process.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON:GG2.GP3	Provide Resources	Provide adequate resources for performing the monitoring process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
MON:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the monitoring process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
MON:GG2.GP5	Train People	Train the people performing or supporting the monitoring process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
MON:GG2.GP6	Control Work Products	Place designated work products of the monitoring process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
MON:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the monitoring process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
MON:GG2.GP8	Measure and Control the Process	Measure and control the monitoring process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
MON:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the monitoring process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
MON:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the monitoring process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
MON:GG3	Institutionalize a Defined Process	Monitoring is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
MON:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined monitoring process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
MON:GG3.GP2	Collect Improvement Information	Collect monitoring work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
OPD:SG1	Establish Organizational Process Assets	A set of organizational process assets is established and maintained.	Functional	Subset Of	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	10	
OPD:SG1.SP1	Establish Standard Processes	The organization's set of standard processes is established and maintained.	Functional	Subset Of	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	10	
OPD:SG1.SP2	Establish Tailoring Criteria and Guidelines	Tailoring criteria and guidelines for the organization's set of standard processes are established and maintained.	Functional	Intersects With	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to:(1) Mission / business functions;(2) Operational environment;(3) Specific threats or vulnerabilities; or(4) Other conditions or situations that could affect mission / business success.	5	
OPD:SG1.SP3	Establish the Organization's Measurement Repository	The organization's measurement repository is established and maintained.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPD:SG1.SP4	Establish the Organization's Process Asset Library	The organization's process asset library is established and maintained.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPD:SG1.SP5	Establish Work Environment Standards	Work environment standards are established and maintained.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPD:SG1.SP6	Establish Rules and Guidelines for Integrated Teams	Organizational rules and guidelines for the structure, formation, and operation of integrated teams are established and maintained.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPD:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Organizational Process Definition process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
OPD:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Organizational Process Definition process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
OPD:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Organizational Process Definition process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPD:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Organizational Process Definition process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
OPD:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Organizational Process Definition process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
OPD:GG2	Institutionalize a Managed Process	Organizational process definition is institutionalized as a managed process.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPD:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the organizational process definition process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
OPD:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the organizational process definition process.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPD:GG2.GP3	Provide Resources	Provide adequate resources for performing the organizational process definition process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
OPD:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the organizational process definition process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
OPD:GG2.GP5	Train People	Train the people performing or supporting the organizational process definition process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
OPD:GG2.GP6	Control Work Products	Place designated work products of the organizational process definition process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
OPD:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the organizational process definition process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
OPD:GG2.GP8	Measure and Control the Process	Measure and control the organizational process definition process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
OPD:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the organizational process definition process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
OPD:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the organizational process definition process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
OPD:GG3	Institutionalize a Defined Process	Organizational process definition is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
OPD:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined organizational process definition process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
OPD:GG3.GP2	Collect Improvement Information	Collect organizational process definition work products, measures, measurement results, and improvement information derived from planning and performing the process to support the future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
OPF:SG1	Determine Process Improvement Opportunities	Strengths, weaknesses, and improvement opportunities for the organization's processes are identified periodically and as needed.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPF:SG1.SP1	Establish Organizational Process Needs	The descriptions of process needs and objectives for the organization are established and maintained.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPF:SG1.SP2	Appraise the Organization's Processes	The organization's processes are appraised periodically and as needed to maintain an understanding of their strengths and weaknesses.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPF:SG1.SP3	Identify the Organization's Process Improvements	Improvements to the organization's processes and process assets are identified.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPF:SG2	Plan and Implement Process Actions	Process actions that address improvements to the organization's processes and process assets are planned and implemented.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPF:SG2.SP1	Establish Process Action Plans	Process action plans to address improvements to the organization's processes and process assets are established and maintained.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPF:SG2.SP2	Implement Process Action Plans	Process action plans are implemented.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPF:SG3	Deploy Organizational Process Assets and Incorporate Experiences	Organizational process assets are deployed across the organization, and process-related experiences are incorporated into organizational process assets.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPF:SG3.SP1	Deploy Organizational Process Assets	Organizational process assets are deployed across the organization.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPF:SG3.SP2	Deploy Standard Processes	The organization's set of standard processes are deployed to organizational units (including projects at their start-up) and changes are deployed to them as appropriate.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPF:SG3.SP3	Monitor the Implementation	The organization's set of standard processes and use of process assets are monitored.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPF:SG3.SP4	Incorporate Experiences into Organizational Process Assets	Process-related work products, measures, and improvement information derived from planning and performing the process are incorporated into organizational process assets.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPF:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Organizational Process Focus process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
OPF:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Organizational Process Focus process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
OPF:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Organizational Process Focus process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPF:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Organizational Process Focus process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
OPF:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Organizational Process Focus process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
OPF:GG2	Institutionalize a Managed Process	Organizational process focus is institutionalized as a managed process.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPF:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the organizational process focus process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
OPF:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the organizational process focus process.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
OPF:GG2.GP3	Provide Resources	Provide adequate resources for performing the organizational process focus process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
OPF:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the organizational process focus process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
OPF:GG2.GP5	Train People	Train the people performing or supporting the organizational process focus process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
OPF:GG2.GP6	Control Work Products	Place designated work products of the organizational process focus process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
OPF:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the organizational process focus process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
OPF:GG2.GP8	Measure and Control the Process	Measure and control the organizational process focus process against the plan for performing the process, and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
OPF:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the organizational process focus process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
OPF:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the organizational process focus process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
OPF:GG3	Institutionalize a Defined Process	Organizational process focus is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
OPF:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined organizational process focus process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
OPF:GG3.GP2	Collect Improvement Information	Collect organizational process focus work products, measures, measurement results, and improvement information derived from planning and performing the process to support the future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
OTA:SG1	Establish Awareness Program	An awareness program that supports the organization's resilience program is established.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:SG1.SP1	Establish Awareness Needs	The awareness needs of the organization are established and maintained.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:SG1.SP2	Establish Awareness Plan	A plan for developing, implementing, and maintaining an awareness program is established and maintained.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:SG1.SP3	Establish Awareness Delivery Capability	A capability for consistent and repeatable delivery of awareness artifacts is established and maintained.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:SG2	Conduct Awareness Activities	Awareness activities that support the organization's resilience program are performed.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:SG2.SP1	Perform Awareness Activities	Awareness activities are performed according to the awareness plan.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:SG2.SP2	Establish Awareness Records	Records of awareness activities performed are established and maintained.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:SG2.SP3	Assess Awareness Program Effectiveness	The effectiveness of the awareness program is assessed and corrective actions are identified.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:SG3	Establish Training Capability	Training capabilities that support the operational resilience management system are established and maintained.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:SG3.SP1	Establish Training Needs	The training needs of the organization are established and maintained.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:SG3.SP2	Establish Training Plan	A plan for developing, implementing, and maintaining a resilience training program is established and maintained.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:SG3.SP3	Establish Training Capability	A capability for delivering training to resilience staff is established and maintained.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:SG4	Conduct Training	Training necessary for staff to perform their roles effectively is provided.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:SG4.SP1	Deliver Resilience Training	Training is delivered according to the training plan.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:SG4.SP2	Establish Training Records	Records of delivered training are established and maintained.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:SG4.SP3	Assess Training Effectiveness	The effectiveness of the training program is assessed and corrective actions are identified.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Organizational Training and Awareness process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
OTA:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Organizational Training and Awareness process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
OTA:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Organizational Training and Awareness process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
OTA:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Organizational Training and Awareness process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
OTA:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Organizational Training and Awareness process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
OTA:GG2	Institutionalize a Managed Process	Organizational training and awareness is institutionalized as a managed process.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the organizational training and awareness process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
OTA:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the organizational training and awareness process.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
OTA:GG2.GP3	Provide Resources	Provide adequate resources for performing the organizational training and awareness process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
OTA:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the organizational training and awareness process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
OTA:GG2.GP5	Train People	Train the people performing or supporting the organizational training and awareness process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
OTA:GG2.GP6	Control Work Products	Place designated work products of the organizational training and awareness process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
OTA:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the organizational training and awareness process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
OTA:GG2.GP8	Measure and Control the Process	Measure and control the organizational training and awareness process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
OTA:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the organizational training and awareness process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
OTA:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the organizational training and awareness process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
OTA:GG3	Institutionalize a Defined Process	Organizational training and awareness is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
OTA:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined organizational training and awareness process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
OTA:GG3.GP2	Collect Improvement Information	Collect organizational training and awareness work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
PM:SG1	Establish Vital Staff	The vital staff of the organization are identified and prioritized.	Functional	Intersects With	Identify Vital Security, Compliance & Resilience Staff	HRS-13.2	Mechanisms exist to identify vital security, compliance and resilience staff.	5	
PM:SG1.SP1	Identify Vital Staff	The vital staff from a resilience perspective are identified and characterized.	Functional	Intersects With	Identify Vital Security, Compliance & Resilience Staff	HRS-13.2	Mechanisms exist to identify vital security, compliance and resilience staff.	5	
PM:SG2	Manage Risks Associated with Staff Availability	Operational risks related to the availability of staff are identified and managed.	Functional	Intersects With	Identify Vital Security, Compliance & Resilience Staff	HRS-13.2	Mechanisms exist to identify vital security, compliance and resilience staff.	5	
PM:SG2.SP1	Identify and Assess Staff Risks	Risks to the availability of staff are periodically identified and assessed.	Functional	Intersects With	Identify Vital Security, Compliance & Resilience Staff	HRS-13.2	Mechanisms exist to identify vital security, compliance and resilience staff.	5	
PM:SG2.SP2	Address Staff Risks	Risk response plans for the risks related to the availability of staff are developed and implemented.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	
PM:SG3	Manage the Availability of Staff	The availability of staff is managed to support high-value services.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
PM:SG3.SP1	Establish Redundancy for Vital Staff	Redundancy for vital staff is established to ensure continuity of services.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
PM:SG3.SP2	Perform Succession Planning	Vital management roles and responsibilities are supported through succession planning.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
PM:SG3.SP3	Prepare for Redeployment	Plans are established and staff are prepared to redeploy to other roles during a disruptive event or in the execution of a service continuity plan.	Functional	Subset Of	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	10	
PM:SG3.SP4	Plan to Support Staff During Disruptive Events	Plans are developed and implemented to ensure support is provided for staff as they are deployed during a disruptive event.	Functional	Subset Of	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	10	
PM:SG3.SP5	Plan for Return-to-Work Considerations	Plans are developed and implemented to address return-to-work issues for staff after a disruptive event.	Functional	Subset Of	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	10	
PM:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the People Management process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
PM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the People Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
PM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the People Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
PM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the People Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
PM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the People Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
PM:GG2	Institutionalize a Managed Process	People management is institutionalized as a managed process.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
PM:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the people management process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
PM:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the people management process.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
PM:GG2.GP3	Provide Resources	Provide adequate resources for performing the people management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
PM:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the people management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
PM:GG2.GP5	Train People	Train the people performing or supporting the people management process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
PM:GG2.GP6	Control Work Products	Place designated work products of the people management process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
PM:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the people management process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
PM:GG2.GP8	Measure and Control the Process	Measure and control the people management process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
PM:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the people management process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
PM:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the people management process with higher level managers, and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
PM:GG3	Institutionalize a Defined Process	People management is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
PM:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined people management process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
PM:GG3.GP2	Collect Improvement Information	Collect people management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
RISK:SG1	Prepare for Risk Management	Preparation for risk management is performed.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RISK:SG1.SP1	Determine Risk Sources and Categories	The sources of risk to assets and services are identified and the categories of risk that are relevant to the organization are determined.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
RISK:SG1.SP2	Establish an Operational Risk Management Strategy	A strategy for managing operational risk relative to strategic objectives is established and maintained.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RISK:SG2	Establish Risk Parameters and Focus	Risk appetite and tolerances are identified and documented and the focus of risk management activities is established.	Functional	Intersects With	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	5	
RISK:SG2.SP1	Define Risk Parameters	The organization's risk parameters are defined.	Functional	Intersects With	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	5	
RISK:SG2.SP2	Establish Risk Measurement Criteria	Criteria for measuring the organizational impact of realized risk are established.	Functional	Intersects With	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	5	
RISK:SG3	Identify Risks	Operational risks are identified.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
RISK:SG3.SP1	Identify Asset-Level Risks	Operational risks that affect assets that support services are identified.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
RISK:SG3.SP2	Identify Service-Level Risks	Operational risks that potentially affect services are identified.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
RISK:SG4	Analyze Risks	Risks are analyzed to determine priority and importance.	Functional	Intersects With	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	5	
RISK:SG4.SP1	Evaluate Risks	Risks are evaluated against risk tolerances and criteria, and the potential impact of risk is characterized.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
RISK:SG4.SP2	Categorize and Prioritize Risks	Risks are categorized and prioritized relative to risk parameters.	Functional	Intersects With	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that:(1) Document the security categorization results (including supporting rationale) in the security plan for systems; and(2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5	
RISK:SG4.SP3	Assign Risk Disposition	The strategy for disposition of each identified risk is established and maintained.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RISK:SG5	Address Risks	Risks to assets and services are addressed to prevent disruption of operational resilience.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
RISK:SG5.SP1	Develop Risk Response Plans	Risk response plans are developed.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	
RISK:SG5.SP2	Implement Risk Strategies and Plans	Risk strategies and response plans are implemented and monitored.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	
RISK:SG6	Use Risk Information to Manage Resilience	Information gathered from identified and realized risk is used to improve the operational resilience management system.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RISK:SG6.SP1	Review and Adjust Strategies to Protect Assets and Services	Protection strategies implemented to protect assets and services from risk are evaluated and updated as required based on risk information.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RISK:SG6.SP2	Review and Adjust Strategies to Sustain Services	Sustainment strategies are developed to ensure services are sustained and plans are evaluated and updated as required based on risk information.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RISK:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the goals of the Risk Management process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
RISK:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Risk Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
RISK:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Risk Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RISK:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Risk Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
RISK:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Risk Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
RISK:GG2	Institutionalize a Managed Process	Risk management is institutionalized as a managed process.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RISK:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the risk management process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
RISK:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the risk management process.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RISK:GG2.GP3	Provide Resources	Provide adequate resources for performing the risk management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
RISK:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the risk management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
RISK:GG2.GP5	Train People	Train the people performing or supporting the risk management process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
RISK:GG2.GP6	Control Work Products	Place designated work products of the risk management process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
RISK:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the risk management process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
RISK:GG2.GP8	Measure and Control the Process	Measure and control the risk management process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
RISK:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the risk management process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
RISK:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the risk management process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
RISK:GG3	Institutionalize a Defined Process	Risk management is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
RISK:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined risk management process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
RISK:GG3.GP2	Collect Improvement Information	Collect risk management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
RRD:SG1	Identify Enterprise Requirements	The organization's enterprise-level resilience requirements are identified and established.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRD:SG1.SP1	Establish Enterprise Resilience Requirements	The resilience requirements of the enterprise are established.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRD:SG2	Develop Service Requirements	The resilience requirements for services are developed and established based on the service mission and the requirements of supporting assets.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRD:SG2.SP1	Establish Asset Resilience Requirements	The resilience requirements of assets as they relate to the services they support are established.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRD:SG2.SP2	Assign Enterprise Resilience Requirements to Services	Enterprise requirements that affect services are assigned to the services.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRD:SG3	Analyze and Validate Requirements	The resilience requirements for services are analyzed and validated.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRD:SG3.SP1	Establish a Definition of Required Functionality	A definition of the required functionality of assets in the context of the services they support is established and maintained.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRD:SG3.SP2	Analyze Resilience Requirements	The requirements of assets are analyzed to identify conflicts, interdependencies, and shared requirements.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRD:SG3.SP3	Validate Resilience Requirements	Asset-level resilience requirements are validated to ensure they adequately specify what is needed to protect and sustain an asset commensurate with its value.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRD:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Resilience Requirements Development process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
RRD:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Resilience Requirements Development process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
RRD:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Resilience Requirements Development process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
RRD:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Resilience Requirements Development process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
RRD:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Resilience Requirements Development process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
RRD:GG2	Institutionalize a Managed Process	Resilience requirements development is institutionalized as a managed process.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRD:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the resilience requirements development process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
RRD:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the resilience requirements development process.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRD:GG2.GP3	Provide Resources	Provide adequate resources for performing the resilience requirements development process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
RRD:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the resilience requirements development process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
RRD:GG2.GP5	Train People	Train the people performing or supporting the resilience requirements development process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
RRD:GG2.GP6	Control Work Products	Place designated work products of the resilience requirements development process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
RRD:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the resilience requirements development process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
RRD:GG2.GP8	Measure and Control the Process	Measure and control the resilience requirements development process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
RRD:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the resilience requirements development process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
RRD:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the resilience requirements development process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
RRD:GG3	Institutionalize a Defined Process	Resilience requirements development is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
RRD:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined resilience requirements development process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
RRD:GG3.GP2	Collect Improvement Information	Collect resilience requirements development work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
RRM:SG1	Manage Requirements	Resilience requirements are actively managed and inconsistencies between requirements and the activities necessary to satisfy them are identified.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRM:SG1.SP1	Obtain an Understanding of Resilience Requirements	An understanding of resilience requirements is obtained from providers to ensure consistency and accuracy.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRM:SG1.SP2	Obtain Commitment to Resilience Requirements	Commitments to resilience requirements are obtained from those who are responsible for satisfying the requirements.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRM:SG1.SP3	Manage Resilience Requirements Changes	Changes to resilience requirements are managed as conditions dictate.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRM:SG1.SP4	Maintain Traceability of Resilience Requirements	Traceability between resilience requirements and the activities performed to satisfy the requirements is established.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRM:SG1.SP5	Identify Inconsistencies Between Resilience Requirements and Activities Performed to Meet the Requirements	Inconsistencies between resilience requirements and the activities performed to satisfy the requirements are identified and managed.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRM:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the goals of the Resilience Requirements Management process area by transforming identifiable input work products to produce identifiable work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
RRM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Resilience Requirements Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
RRM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Resilience Requirements Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
RRM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Resilience Requirements Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
RRM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Resilience Requirements Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
RRM:GG2	Institutionalize a Managed Process	Resilience requirements management is institutionalized as a managed process.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRM:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the resilience requirements management process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
RRM:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the resilience requirements management process.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RRM:GG2.GP3	Provide Resources	Provide adequate resources for performing the resilience requirements management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
RRM:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the resilience requirements management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
RRM:GG2.GP5	Train People	Train the people performing or supporting the resilience requirements management process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
RRM:GG2.GP6	Control Work Products	Place designated work products of the resilience requirements management process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
RRM:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the resilience requirements management process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
RRM:GG2.GP8	Measure and Control the Process	Measure and control the resilience requirements management process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
RRM:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the resilience requirements management process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
RRM:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the resilience requirements management process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
RRM:GG3	Institutionalize a Defined Process	Resilience requirements management is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
RRM:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined resilience requirements management process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
RRM:GG3.GP2	Collect Improvement Information	Collect resilience requirements management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
RTSE:SG1	Establish Guidelines for Resilient Technical Solution Development	Guidelines are developed to ensure proper consideration of resilience activities and controls in all phases of the life cycle.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
RTSE:SG1.SP1	Identify General Guidelines	General guidelines for building resilience into software and systems are identified.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
RTSE:SG1.SP2	Identify Requirements Guidelines	Guidelines for determining software and systems resilience requirements are identified.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
RTSE:SG1.SP3	Identify Architecture and Design Guidelines	Guidelines for designing resilience into software and systems are identified.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
RTSE:SG1.SP4	Identify Implementation Guidelines	Guidelines for implementing resilient software and systems are identified.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
RTSE:SG1.SP5	Identify Assembly and Integration Guidelines	Guidelines for the assembly and integration of resilient software into resilient systems are identified.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
RTSE:SG2	Develop Resilient Technical Solution Development Plans	Plans for addressing resilience in the development life cycle are based on documented guidelines.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
RTSE:SG2.SP1	Select and Tailor Guidelines	Guidelines are determined for a specific software or system development project using selection criteria.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
RTSE:SG2.SP2	Integrate Selected Guidelines with a Defined Software and System Development Process	Selected resilience guidelines are integrated with a defined software and system development process and a documented plan.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
RTSE:SG3	Execute the Plan	Progress against the plan for developing resilient software and systems is monitored throughout the development life cycle.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
RTSE:SG3.SP1	Monitor Execution of the Development Plan	Execution of the development plan is monitored to ensure that software and system resilience requirements are satisfied.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RTSE:SG3.SP2	Release Resilient Technical Solutions into Production	Software and systems that demonstrate satisfaction of resilience requirements are released into production.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
RTSE:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Resilient Technical Solution Engineering process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
RTSE:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Resilient Technical Solution Engineering process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
RTSE:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Resilient Technical Solution Engineering process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
RTSE:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Resilient Technical Solution Engineering process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
RTSE:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Resilient Technical Solution Engineering process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
RTSE:GG2	Institutionalize a Managed Process	Resilient technical solution engineering is institutionalized as a managed process.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
RTSE:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the resilient technical solution engineering process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
RTSE:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the resilient technical solution engineering process.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
RTSE:GG2.GP3	Provide Resources	Provide adequate resources for performing the resilient technical solution engineering process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
RTSE:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the resilient technical solution engineering process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
RTSE:GG2.GP5	Train People	Train the people performing or supporting the resilient technical solution engineering process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
RTSE:GG2.GP6	Control Work Products	Place designated work products of the resilient technical solution engineering process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
RTSE:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the resilient technical solution engineering process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
RTSE:GG2.GP8	Measure and Control the Process	Measure and control the resilient technical solution engineering process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
RTSE:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the resilient technical solution engineering process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
RTSE:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the resilient technical solution engineering process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
RTSE:GG3	Institutionalize a Defined Process	Resilient technical solution engineering is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
RTSE:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined resilient technical solution engineering process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
RTSE:GG3.GP2	Collect Improvement Information	Collect resilient technical solution engineering work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
SC:SG1	Prepare for Service Continuity	The organizational processes for sustainability planning and execution are established.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
SC:SG1.SP1	Plan for Service Continuity	Planning is performed for developing and implementing the organization's service continuity process.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
SC:SG1.SP2	Establish Standards and Guidelines for Service Continuity	The guidelines and standards for service continuity are established and communicated.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
SC:SG2	Identify and Prioritize High-Value Services	The services that are required to meet the organization's mission are identified and prioritized.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
SC:SG2.SP1	Identify the Organization's High-Value Services	The high-value services of the organization and their associated assets are identified.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
SC:SG2.SP2	Identify Internal and External Dependencies and Interdependencies	The internal and external relationships necessary to ensure service continuity are identified and analyzed.	Functional	Subset Of	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	10	
SC:SG2.SP3	Identify Vital Organizational Records and Databases	Vital information required for service continuity is identified.	Functional	Subset Of	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	10	
SC:SG3	Develop Service Continuity Plans	Service continuity plans for high-value organizational services are developed.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
SC:SG3.SP1	Identify Plans to Be Developed	Required service continuity plans are identified.	Functional	Subset Of	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	10	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SC:SG3.SP2	Develop and Document Service Continuity Plans	The required service continuity plans are developed and documented.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG3.SP3	Assign Staff to Service Continuity Plans	Staff members are assigned to the service continuity plans to ensure effective execution.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG3.SP4	Store and Secure Service Continuity Plans	Service continuity plans are stored and made accessible to those with a need to know.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG3.SP5	Develop Service Continuity Plan Training	Training in the service continuity plans is developed and administered.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG4	Validate Service Continuity Plans	Service continuity plans are validated to ensure they satisfy standards and guidelines and to resolve conflicts between plans.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG4.SP1	Validate Plans to Requirements and Standards	Service continuity plans are examined to ensure they satisfy standards and guidelines.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG4.SP2	Identify and Resolve Plan Conflicts	Conflicts between service continuity plans are identified and resolved.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG5	Exercise Service Continuity Plans	Service continuity plans are exercised to ensure they meet their stated objectives.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG5.SP1	Develop Testing Program and Standards	A program and standards for service continuity plan testing are established and implemented.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG5.SP2	Develop and Document Test Plans	Service continuity test plans are developed and documented.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG5.SP3	Exercise Plans	Service continuity plans are exercised on a regular basis and results are documented.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG5.SP4	Evaluate Plan Test Results	Opportunities for improving service continuity are identified and implemented as a result of exercising.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG6	Execute Service Continuity Plans	Service continuity plans are executed and reviewed.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG6.SP1	Execute Plans	Service continuity plans are executed as required.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG6.SP2	Measure the Effectiveness of the Plans in Operation	Post-execution review is performed to identify corrective actions.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG7	Maintain Service Continuity Plans	Changes to service continuity plans are identified and managed.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG7.SP1	Establish Change Criteria	Change criteria for service continuity plans are established.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:SG7.SP2	Maintain Changes to Plans	Changes are made to service continuity plans as conditions dictate.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Service Continuity process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
SC:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Service Continuity process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
SC:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Service Continuity process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Service Continuity process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
SC:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Service Continuity process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
SC:GG2	Institutionalize a Managed Process	Service continuity is institutionalized as a managed process.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the service continuity process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
SC:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the service continuity process.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
SC:GG2.GP3	Provide Resources	Provide adequate resources for performing the service continuity process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
SC:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the service continuity process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
SC:GG2.GP5	Train People	Train the people performing or supporting the service continuity process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
SC:GG2.GP6	Control Work Products	Place designated work products of the service continuity process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
SC:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the service continuity process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
SC:GG2.GP8	Measure and Control the Process	Measure and control the service continuity process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
SC:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the service continuity process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
SC:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the service continuity process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
SC:GG3	Institutionalize a Defined Process	Service continuity is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
SC:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined service continuity process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
SC:GG3.GP2	Collect Improvement Information	Collect service continuity work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
TM:SG1	Establish and Prioritize Technology Assets	Technology assets are prioritized to ensure the resilience of the high-value services that they support.	Functional	Intersects With	Asset Categorization	AST-31	Mechanisms exist to categorize Technology Assets, Applications and/or Services (TAAS).	5	
TM:SG1.SP1	Prioritize Technology Assets	Technology assets are prioritized relative to their importance in supporting the delivery of high-value services.	Functional	Intersects With	Asset Categorization	AST-31	Mechanisms exist to categorize Technology Assets, Applications and/or Services (TAAS).	5	
TM:SG1.SP2	Establish Resilience-Focused Technology Assets	Technology assets that specifically support execution of service continuity plans are identified and established.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
TM:SG2	Protect Technology Assets	Administrative, technical, and physical controls for technology assets are identified, implemented, monitored, and managed.	Functional	Subset Of	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
TM:SG2.SP1	Assign Resilience Requirements to Technology Assets	Resilience requirements that have been defined are assigned to technology assets.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to:(1) Unintentional errors (by users or software); and(2) Intentional attack or circumvention.	5	
TM:SG2.SP2	Establish and Implement Controls	Administrative, technical, and physical controls that are required to meet the established resilience requirements are identified and implemented.	Functional	Subset Of	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
TM:SG3	Manage Technology Asset Risks	Operational risks to technology assets are identified and managed.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
TM:SG3.SP1	Identify and Assess Technology Asset Risks	Risks to technology assets are identified and assessed.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
TM:SG3.SP2	Address Technology Asset Risks	Risk response plans for risks to technology assets are developed and implemented.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	
TM:SG4	Manage Technology Asset Integrity	The integrity of technology assets is managed.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
TM:SG4.SP1	Control Access to Technology Assets	Access to technology assets is controlled.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
TM:SG4.SP2	Perform Configuration Management	The configuration of technology assets is managed.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
TM:SG4.SP3	Perform Change Control and Management	Changes to technology assets are managed.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
TM:SG4.SP4	Perform Release Management	The iteration of technology assets placed into the production environment is managed.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
TM:SG5	Manage Technology Asset Availability	The availability of technology assets to support high-value services is managed.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
TM:SG5.SP1	Perform Planning to Sustain Technology Assets	The availability and functionality of high-value technology assets are ensured through developing plans to sustain them.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
TM:SG5.SP2	Manage Technology Asset Maintenance	Operational maintenance is performed on technology assets.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
TM:SG5.SP3	Manage Technology Capacity	The operating capacity of technology assets is managed.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
TM:SG5.SP4	Manage Technology Interoperability	The interoperability of technology assets is managed.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
TM:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Technology Management process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
TM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Technology Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
TM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Technology Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
TM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Technology Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
TM:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Technology Management process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
TM:GG2	Institutionalize a Managed Process	Technology management is institutionalized as a managed process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
TM:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the technology management process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
TM:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the technology management process.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
TM:GG2.GP3	Provide Resources	Provide adequate resources for performing the technology management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
TM:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the technology management process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
TM:GG2.GP5	Train People	Train the people performing or supporting the technology management process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
TM:GG2.GP6	Control Work Products	Place designated work products of the technology management process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
TM:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the technology management process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
TM:GG2.GP8	Measure and Control the Process	Measure and control the technology management process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
TM:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the technology management process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
TM:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the technology management process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
TM:GG3	Institutionalize a Defined Process	Technology management is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
TM:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined technology management process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
TM:GG3.GP2	Collect Improvement Information	Collect technology management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
VAR:SG1	Prepare for Vulnerability Analysis and Resolution	Preparation for vulnerability analysis and resolution activities is conducted.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
VAR:SG1.SP1	Establish Scope	The assets and operational environments that must be examined for vulnerabilities are identified.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
VAR:SG1.SP2	Establish a Vulnerability Analysis and Resolution Strategy	An operational vulnerability analysis and resolution strategy is established and maintained.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
VAR:SG2	Identify and Analyze Vulnerabilities	A process for identifying and analyzing vulnerabilities is established and maintained.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
VAR:SG2.SP1	Identify Sources of Vulnerability Information	The sources of vulnerability information are identified.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
VAR:SG2.SP2	Discover Vulnerabilities	A process is established to actively discover vulnerabilities.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
VAR:SG2.SP3	Analyze Vulnerabilities	Vulnerabilities are analyzed to determine whether they have to be reduced or eliminated.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
VAR:SG3	Manage Exposure to Vulnerabilities	Strategies are developed to manage exposure to identified vulnerabilities.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
VAR:SG3.SP1	Manage Exposure to Vulnerabilities	Strategies are developed and implemented to manage exposure to identified vulnerabilities.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
VAR:SG4	Identify Root Causes	The root causes of vulnerabilities are examined to improve vulnerability analysis and resolution and reduce organizational exposure.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
VAR:SG4.SP1	Perform Root-Cause Analysis	A review of identified vulnerabilities is performed to determine and address underlying causes.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
VAR:GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the Vulnerability Analysis and Resolution process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
VAR:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Vulnerability Analysis and Resolution process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
VAR:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Vulnerability Analysis and Resolution process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
VAR:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Vulnerability Analysis and Resolution process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
VAR:GG1.GP1	Perform Specific Practices	Perform the specific practices of the Vulnerability Analysis and Resolution process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
VAR:GG2	Institutionalize a Managed Process	Vulnerability analysis and resolution is institutionalized as a managed process.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
VAR:GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the vulnerability analysis and resolution process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
VAR:GG2.GP2	Plan the Process	Establish and maintain the plan for performing the vulnerability analysis and resolution process.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
VAR:GG2.GP3	Provide Resources	Provide adequate resources for performing the vulnerability analysis and resolution process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
VAR:GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the vulnerability analysis and resolution process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
VAR:GG2.GP5	Train People	Train the people performing or supporting the vulnerability analysis and resolution process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
VAR:GG2.GP6	Control Work Products	Place designated work products of the vulnerability analysis and resolution process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
VAR:GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the vulnerability analysis and resolution process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
VAR:GG2.GP8	Measure and Control the Process	Measure and control the vulnerability analysis and resolution process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
VAR:GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the vulnerability analysis and resolution process against its process description, standards, and procedures, and address non-compliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
VAR:GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the vulnerability analysis and resolution process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
VAR:GG3	Institutionalize a Defined Process	Vulnerability analysis and resolution is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
VAR:GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined vulnerability analysis and resolution process.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
VAR:GG3.GP2	Collect Improvement Information	Collect vulnerability analysis and resolution work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
GG1	Achieve Specific Goals	The operational resilience management system supports and enables achievement of the specific goals of the process area by transforming identifiable input work products to produce identifiable output work products.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
GG1.GP1	Perform Specific Practices	Perform the specific practices of the process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	
GG1.GP1	Perform Specific Practices	Perform the specific practices of the process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
GG1.GP1	Perform Specific Practices	Perform the specific practices of the process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
GG1.GP1	Perform Specific Practices	Perform the specific practices of the process area to develop work products and provide services to achieve the specific goals of the process area.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
GG2	Institutionalize a Managed Process	The process is institutionalized as a managed process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
GG2.GP1	Establish Process Governance	Establish and maintain governance over the planning and performance of the process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
GG2.GP2	Plan the Process	Establish and maintain the plan for performing the process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
GG2.GP3	Provide Resources	Provide adequate resources for performing the process, developing the work products, and providing the services of the process.	Functional	Subset Of	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
GG2.GP4	Assign Responsibility	Assign responsibility and authority for performing the process, developing the work products, and providing the services of the process.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
GG2.GP5	Train People	Train the people performing or supporting the process as needed.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	10	
GG2.GP6	Control Work Products	Place designated work products of the process under appropriate levels of control.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
GG2.GP7	Identify and Involve Relevant Stakeholders	Identify and involve the relevant stakeholders of the process as planned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
GG2.GP8	Measure and Control the Process	Measure and control the process against the plan for performing the process and take appropriate corrective action.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
GG2.GP9	Objectively Evaluate Adherence	Objectively evaluate adherence of the process against its process description, standards, and procedures, and address noncompliance.	Functional	Intersects With	Assessment Objectives (AO)	GOV-19.2	Mechanisms exist to utilize defined Assessment Objectives (AO) to assess the implementation of requirements, when available.	5	
GG2.GP10	Review Status with Higher Level Managers	Review the activities, status, and results of the process with higher level managers and resolve issues.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
GG3	Institutionalize a Defined Process	The process is institutionalized as a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
GG3.GP1	Establish a Defined Process	Establish and maintain the description of a defined process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
GG3.GP2	Collect Improvement Information	Collect work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	Functional	Intersects With	Work Products	CPL-13	Mechanisms exist to produce work products (e.g., process artifacts) that demonstrate the ability to comply with applicable requirements.	5	