NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Cybersecurity Capability Maturity Model (C2M2) Version 2.1
Focal Document URL: https://c2m2.doe.gov/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-doe-c2m2-2-1.pdf

FDE #	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
ASSET-1a	ASSET-1.a	N/A	IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner	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.	8	
ASSET-1a	ASSET-1.a	N/A	IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner	Functional	Intersects With	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.	8	
ASSET-1b	ASSET-1.b	N/A	The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective	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	
ASSET-1c	ASSET-1.c	N/A	Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function	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	
ASSET-1c	ASSET-1.c	N/A	Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	
ASSET-1d	ASSET-1.d	N/A	Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective	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	
ASSET-1d	ASSET-1.d	N/A	Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective	Functional	Intersects With	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.	5	
ASSET-1d	ASSET-1.d	N/A	Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective	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	
ASSET-1d	ASSET-1.d	N/A	Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	
ASSET-1e	ASSET-1.e	N/A	The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, asset owner, operating system, and firmware versions)	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	
ASSET-1f	ASSET-1.f	N/A	The IT and OT asset inventory is complete (the inventory includes all assets within the function)	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	
ASSET-1g	ASSET-1.g	N/A	The IT and OT asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes	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	
ASSET-1h	ASSET-1.h	N/A	Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life	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	
ASSET-1h	ASSET-1.h	N/A	Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	8	
ASSET-1h	ASSET-1.h	N/A	Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	8	
ASSET-2a	ASSET-2.a	N/A	Information assets that are important to the delivery of the function (for example, SCADA set points and customer information) are inventoried, at least in an ad hoc manner	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	
ASSET-2b	ASSET-2.b	N/A	The information asset inventory includes information assets within the function that may be leveraged to achieve a threat objective	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	
ASSET-2c	ASSET-2.c	N/A	Inventoried information assets are categorized based on defined criteria that includes importance to the delivery of the function	Functional	Intersects With	Asset Categorization	AST-31	Mechanisms exist to categorize Technology Assets, Applications and/or Services (TAAS).	8	
ASSET-2c	ASSET-2.c	N/A	Inventoried information assets are categorized based on defined criteria that includes importance to the delivery of the function	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.	8	
ASSET-2c	ASSET-2.c	N/A	Inventoried information assets are categorized based on defined criteria that includes importance to the delivery of the function	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	8	
ASSET-2d	ASSET-2.d	N/A	Categorization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective	Functional	Intersects With	Asset Categorization	AST-31	Mechanisms exist to categorize Technology Assets, Applications and/or Services (TAAS).	8	
ASSET-2d	ASSET-2.d	N/A	Categorization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	8	
ASSET-2d	ASSET-2.d	N/A	Categorization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective	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.	8	
ASSET-2e	ASSET-2.e	N/A	The information asset inventory includes attributes that support cybersecurity activities (for example, asset category, backup locations and frequencies, storage locations, asset owner, cybersecurity requirements)	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	
ASSET-2e	ASSET-2.e	N/A	The information asset inventory includes attributes that support cybersecurity activities (for example, asset category, backup locations and frequencies, storage locations, asset owner, cybersecurity requirements)	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.	8	
ASSET-2f	ASSET-2.f	N/A	The information asset inventory is complete (the inventory includes all assets within the function)	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	
ASSET-2g	ASSET-2.g	N/A	The information asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes	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	
ASSET-2g	ASSET-2.g	N/A	The information asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes	Functional	Intersects With	Updates During Installations / Removals	AST-02.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.	5	
ASSET-2g	ASSET-2.g	N/A	The information asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes	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	
ASSET-2h	ASSET-2.h	N/A	Information assets are sanitized or destroyed at end of life using techniques appropriate to their cybersecurity requirements	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	8	

FDE #	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
ASSET-2h	ASSET-2.h	N/A	Information assets are sanitized or destroyed at end of life using techniques appropriate to their cybersecurity requirements	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	8	
ASSET-3a	ASSET-3.a	N/A	Configuration baselines are established, at least in an ad hoc manner	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
ASSET-3b	ASSET-3.b	N/A	Configuration baselines are used to configure assets at deployment and restoration	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
ASSET-3c	ASSET-3.c	N/A	Configuration baselines incorporate applicable requirements from the cybersecurity architecture (ARCHITECTURE-1f)	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
ASSET-3d	ASSET-3.d	N/A	Configuration baselines are reviewed and updated periodically and according to defined triggers, such as system changes and changes to the cybersecurity architecture	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations:(1) At least annually;(2) When required due to so; or(3) As part of system component installations and upgrades.	8	
ASSET-3d	ASSET-3.d	N/A	Configuration baselines are reviewed and updated periodically and according to defined triggers, such as system changes and changes to the cybersecurity architecture	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.	8	
ASSET-3e	ASSET-3.e	N/A	Asset configurations are monitored for consistency with baselines throughout the assets' lifecycles	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations:(1) At least annually;(2) When required due to so; or(3) As part of system component installations and upgrades.	5	
ASSET-3e	ASSET-3.e	N/A	Asset configurations are monitored for consistency with baselines throughout the assets' lifecycles	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
ASSET-4a	ASSET-4.a	N/A	Changes to assets are evaluated and approved before being implemented, at least in an ad hoc manner	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
ASSET-4b	ASSET-4.b	N/A	Changes to assets are documented, at least in an ad hoc manner	Functional	Subset Of	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	10	
ASSET-4b	ASSET-4.b	N/A	Changes to assets are documented, at least in an ad hoc manner	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	8	
ASSET-4c	ASSET-4.c	N/A	Documentation requirements for asset changes are established and maintained	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
ASSET-4c	ASSET-4.c	N/A	Documentation requirements for asset changes are established and maintained	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	8	
ASSET-4c	ASSET-4.c	N/A	Documentation requirements for asset changes are established and maintained	Functional	Intersects With	Security, Compliance & Resilience Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.	8	
ASSET-4c	ASSET-4.c	N/A	Documentation requirements for asset changes are established and maintained	Functional	Intersects With	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	8	
ASSET-4d	ASSET-4.d	N/A	Changes to higher priority assets are tested prior to being deployed	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	8	
ASSET-4d	ASSET-4.d	N/A	Changes to higher priority assets are tested prior to being deployed	Functional	Intersects With	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	8	
ASSET-4e	ASSET-4.e	N/A	Changes and updates are implemented in a secure manner	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	8	
ASSET-4e	ASSET-4.e	N/A	Changes and updates are implemented in a secure manner	Functional	Intersects With	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.	8	
ASSET-4e	ASSET-4.e	N/A	Changes and updates are implemented in a secure manner	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	8	
ASSET-4f	ASSET-4.f	N/A	The capability to reverse changes is established and maintained for assets that are important to the delivery of the function	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	8	
ASSET-4f	ASSET-4.f	N/A	The capability to reverse changes is established and maintained for assets that are important to the delivery of the function	Functional	Intersects With	Emergency Changes	CHG-07	Mechanisms exist to govern change management procedures for "emergency" changes.	3	
ASSET-4g	ASSET-4.g	N/A	Change management practices address the full lifecycle of assets (for example, acquisition, deployment, operation, retirement)	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
ASSET-4h	ASSET-4.h	N/A	Changes to higher priority assets are tested for cybersecurity impact prior to being deployed	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	8	
ASSET-4i	ASSET-4.i	N/A	Change logs include information about modifications that impact the cybersecurity requirements of assets	Functional	Subset Of	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	10	
ASSET-5a	ASSET-5.a	N/A	Documented procedures are established, followed, and maintained for activities in the ASSET domain	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	
ASSET-5b	ASSET-5.b	N/A	Adequate resources (people, funding, and tools) are provided to support activities in the ASSET domain	Functional	Subset Of	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	
ASSET-5c	ASSET-5.c	N/A	Up-to-date policies or other organizational directives define requirements for activities in the ASSET domain	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
ASSET-5d	ASSET-5.d	N/A	Responsibility, accountability, and authority for the performance of activities in the ASSET domain are assigned to personnel	Functional	Subset Of	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	10	
ASSET-5e	ASSET-5.e	N/A	Personnel performing activities in the ASSET domain have the skills and knowledge needed to perform their assigned responsibilities	Functional	Subset Of	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	10	
ASSET-5f	ASSET-5.f	N/A	The effectiveness of activities in the ASSET domain is evaluated and tracked	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	10	
THREAT-1a	THREAT-1.a	N/A	Information sources to support cybersecurity vulnerability discovery are identified, at least in an ad hoc manner	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	8	
THREAT-1a	THREAT-1.a	N/A	Information sources to support cybersecurity vulnerability discovery are identified, at least in an ad hoc manner	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	8	
THREAT-1b	THREAT-1.b	N/A	Cybersecurity vulnerability information is gathered and interpreted for the function, at least in an ad hoc manner	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	8	
THREAT-1b	THREAT-1.b	N/A	Cybersecurity vulnerability information is gathered and interpreted for the function, at least in an ad hoc manner	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	
THREAT-1b	THREAT-1.b	N/A	Cybersecurity vulnerability information is gathered and interpreted for the function, at least in an ad hoc manner	Functional	Intersects With	Vulnerability Exploitation Analysis	VPM-03.1	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.	5	
THREAT-1c	THREAT-1.c	N/A	Cybersecurity vulnerability assessments are performed, at least in an ad hoc manner	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	
THREAT-1d	THREAT-1.d	N/A	Cybersecurity vulnerabilities that are relevant to the delivery of the function are mitigated, at least in an ad hoc manner	Functional	Subset Of	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	10	
THREAT-1e	THREAT-1.e	N/A	Cybersecurity vulnerability information sources that collectively address higher priority assets are monitored	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	8	
THREAT-1e	THREAT-1.e	N/A	Cybersecurity vulnerability information sources that collectively address higher priority assets are monitored	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	8	
THREAT-1e	THREAT-1.e	N/A	Cybersecurity vulnerability information sources that collectively address higher priority assets are monitored	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	8	
THREAT-1e	THREAT-1.e	N/A	Cybersecurity vulnerability information sources that collectively address higher priority assets are monitored	Functional	Intersects With	Breadth / Depth of Coverage	VPM-06.2	Mechanisms exist to identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for.	5	
THREAT-1f	THREAT-1.f	N/A	Cybersecurity vulnerability assessments are performed periodically and according to defined triggers, such as system changes and external events	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
THREAT-1g	THREAT-1.g	N/A	Identified cybersecurity vulnerabilities are analyzed and prioritized, and are addressed accordingly	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	8	
THREAT-1g	THREAT-1.g	N/A	Identified cybersecurity vulnerabilities are analyzed and prioritized, and are addressed accordingly	Functional	Intersects With	Vulnerability Exploitation Analysis	VPM-03.1	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.	8	
THREAT-1h	THREAT-1.h	N/A	Operational impact to the function is evaluated prior to deploying patches or other mitigations	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	8	
THREAT-1h	THREAT-1.h	N/A	Operational impact to the function is evaluated prior to deploying patches or other mitigations	Functional	Intersects With	Security, Compliance & Resilience Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.	8	
THREAT-1h	THREAT-1.h	N/A	Operational impact to the function is evaluated prior to deploying patches or other mitigations	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	3	
THREAT-1h	THREAT-1.h	N/A	Operational impact to the function is evaluated prior to deploying patches or other mitigations	Functional	Intersects With	Vulnerability Exploitation Analysis	VPM-03.1	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.	3	
THREAT-1i	THREAT-1.i	N/A	Information on discovered cybersecurity vulnerabilities is shared with organization-defined stakeholders	Functional	Intersects With	Threat Intelligence Reporting	THR-03.1	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	5	
THREAT-1i	THREAT-1.i	N/A	Information on discovered cybersecurity vulnerabilities is shared with organization-defined stakeholders	Functional	Subset Of	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	10	
THREAT-1i	THREAT-1.i	N/A	Information on discovered cybersecurity vulnerabilities is shared with organization-defined stakeholders	Functional	Intersects With	Time To Remediate / Benchmarks For Corrective Action	VPM-05.3	Mechanisms exist to track the effectiveness of remediation operations through metrics reporting.	3	
THREAT-1j	THREAT-1.j	N/A	Cybersecurity vulnerability information sources that collectively address all IT and OT assets within the function are monitored	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
THREAT-1k	THREAT-1.k	N/A	Cybersecurity vulnerability assessments are performed by parties that are independent of the operations of the function	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
THREAT-1l	THREAT-1.l	N/A	Vulnerability monitoring activities include review to confirm that actions taken in response to cybersecurity vulnerabilities were effective	Functional	Subset Of	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	10	
THREAT-1m	THREAT-1.m	N/A	Mechanisms are established and maintained to receive and respond to reports from the public or external parties of potential vulnerabilities related to the organization's IT and OT assets, such as public-facing websites or mobile applications	Functional	Subset Of	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	10	
THREAT-2a	THREAT-2.a	N/A	Internal and external information sources to support threat management activities are identified, at least in an ad hoc manner	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
THREAT-2a	THREAT-2.a	N/A	Internal and external information sources to support threat management activities are identified, at least in an ad hoc manner	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	

FDE #	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
THREAT-2a	THREAT-2.a	N/A	Internal and external information sources to support threat management activities are identified, at least in an ad hoc manner	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	8	
THREAT-2b	THREAT-2.b	N/A	Information about cybersecurity threats is gathered and interpreted for the function, at least in an ad hoc manner	Functional	Intersects With	Threat Intelligence Reporting	THR-03.1	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	8	
THREAT-2b	THREAT-2.b	N/A	Information about cybersecurity threats is gathered and interpreted for the function, at least in an ad hoc manner	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	8	
THREAT-2b	THREAT-2.b	N/A	Information about cybersecurity threats is gathered and interpreted for the function, at least in an ad hoc manner	Functional	Intersects With	Vulnerability Exploitation Analysis	VPM-03.1	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.	8	
THREAT-2c	THREAT-2.c	N/A	Threat objectives for the function are identified, at least in an ad hoc manner	Functional	Subset Of	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	10	
THREAT-2d	THREAT-2.d	N/A	Threats that are relevant to the delivery of the function are addressed, at least in an ad hoc manner	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	8	
THREAT-2d	THREAT-2.d	N/A	Threats that are relevant to the delivery of the function are addressed, at least in an ad hoc manner	Functional	Subset Of	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	10	
THREAT-2e	THREAT-2.e	N/A	A threat profile for the function is established that includes threat objectives and additional threat characteristics (for example, threat actor types, motives, capabilities, and targets)	Functional	Subset Of	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	10	
THREAT-2f	THREAT-2.f	N/A	Threat information sources that collectively address all components of the threat profile are prioritized and monitored	Functional	Subset Of	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	10	
THREAT-2g	THREAT-2.g	N/A	Identified threats are analyzed and prioritized and are addressed accordingly	Functional	Subset Of	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	10	
THREAT-2h	THREAT-2.h	N/A	Threat information is exchanged with stakeholders (for example, executives, operations staff, government, connected organizations, vendors, sector organizations, regulators, Information Sharing and Analysis Centers [ISACs])	Functional	Intersects With	Threat Intelligence Reporting	THR-03.1	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	8	
THREAT-2i	THREAT-2.i	N/A	The threat profile for the function is updated periodically and according to defined triggers, such as system changes and external events	Functional	Intersects With	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5	
THREAT-2j	THREAT-2.j	N/A	Threat monitoring and response activities leverage and trigger predefined states of operation (SITUATION-3g)	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	8	
THREAT-2k	THREAT-2.k	N/A	Secure, near-real-time methods are used for receiving and sharing threat information to enable rapid analysis and action	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	8	
THREAT-2k	THREAT-2.k	N/A	Secure, near-real-time methods are used for receiving and sharing threat information to enable rapid analysis and action	Functional	Intersects With	Threat Intelligence Reporting	THR-03.1	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	8	
THREAT-3a	THREAT-3.a	N/A	Documented procedures are established, followed, and maintained for activities in the THREAT domain	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	
THREAT-3b	THREAT-3.b	N/A	Adequate resources (people, funding, and tools) are provided to support activities in the THREAT domain	Functional	Subset Of	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	
THREAT-3c	THREAT-3.c	N/A	Up-to-date policies or other organizational directives define requirements for activities in the THREAT domain	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
THREAT-3d	THREAT-3.d	N/A	Responsibility, accountability, and authority for the performance of activities in the THREAT domain are assigned to personnel	Functional	Subset Of	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	10	
THREAT-3e	THREAT-3.e	N/A	Personnel performing activities in the THREAT domain have the skills and knowledge needed to perform their assigned responsibilities	Functional	Subset Of	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	10	
THREAT-3f	THREAT-3.f	N/A	The effectiveness of activities in the THREAT domain is evaluated and tracked	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	10	
RISK-1a	RISK-1.a	N/A	The organization has a strategy for cyber risk management, which may be developed and managed in an ad hoc manner	Functional	Subset Of	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.	10	
RISK-1b	RISK-1.b	N/A	A strategy for cyber risk management is established and maintained in alignment with the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
RISK-1c	RISK-1.c	N/A	The cyber risk management program is established and maintained to perform cyber risk management activities according to the cyber risk management strategy	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RISK-1d	RISK-1.d	N/A	Information from RISK domain activities is communicated to relevant stakeholders	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RISK-1e	RISK-1.e	N/A	Governance for the cyber risk management program is established and maintained	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 (TASD)-related risks.	8	
RISK-1e	RISK-1.e	N/A	Governance for the cyber risk management program is established and maintained	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing Technology Assets, Applications, Services and/or Data (TASD)-related risks.	8	
RISK-1f	RISK-1.f	N/A	Senior management sponsorship for the cyber risk management program is visible and active	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	
RISK-1f	RISK-1.f	N/A	Senior management sponsorship for the cyber risk management program is visible and active	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.	8	
RISK-1g	RISK-1.g	N/A	The cyber risk management program aligns with the organization's mission and objectives	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RISK-1h	RISK-1.h	N/A	The cyber risk management program is coordinated with the organization's enterprise-wide risk management program	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RISK-2a	RISK-2.a	N/A	Cyber risks are identified, at least in an ad hoc manner	Functional	Subset Of	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	10	
RISK-2b	RISK-2.b	N/A	A defined method is used to identify cyber risks	Functional	Subset Of	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	10	
RISK-2c	RISK-2.c	N/A	Stakeholders from appropriate operations and business areas participate in the identification of cyber risks	Functional	Subset Of	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	10	
RISK-2d	RISK-2.d	N/A	Identified cyber risks are consolidated into categories (for example, data breaches, insider mistakes, ransomware, OT control takeover) to facilitate management at the category level	Functional	Subset Of	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.	10	
RISK-2e	RISK-2.e	N/A	Cyber risk categories and cyber risks are documented in a risk register or other artifact	Functional	Intersects With	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	
RISK-2e	RISK-2.e	N/A	Cyber risk categories and cyber risks are documented in a risk register or other artifact	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	8	
RISK-2f	RISK-2.f	N/A	Cyber risk categories and cyber risks are assigned to risk owners	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
RISK-2g	RISK-2.g	N/A	Cyber risk identification activities are performed periodically and according to defined triggers, such as system changes and external events	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
RISK-2g	RISK-2.g	N/A	Cyber risk identification activities are performed periodically and according to defined triggers, such as system changes and external events	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-2g	RISK-2.g	N/A	Cyber risk identification activities are performed periodically and according to defined triggers, such as system changes and external events	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-2h	RISK-2.h	N/A	Cyber risk identification activities leverage asset inventory and prioritization information from the ASSET domain, such as IT and OT asset end of support, single points of failure, information asset risk of disclosure, tampering, or destruction	Functional	Intersects With	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.	5	
RISK-2h	RISK-2.h	N/A	Cyber risk identification activities leverage asset inventory and prioritization information from the ASSET domain, such as IT and OT asset end of support, single points of failure, information asset risk of disclosure, tampering, or destruction	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	
RISK-2h	RISK-2.h	N/A	Cyber risk identification activities leverage asset inventory and prioritization information from the ASSET domain, such as IT and OT asset end of support, single points of failure, information asset risk of disclosure, tampering, or destruction	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	
RISK-2i	RISK-2.i	N/A	Vulnerability management information from THREAT domain activities is used to update cyber risks and identify new risks (such as risks arising from vulnerabilities that pose an ongoing risk to the organization or newly identified vulnerabilities)	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-2j	RISK-2.j	N/A	Threat management information from THREAT domain activities is used to update cyber risks and identify new risks	Functional	Intersects With	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	8	
RISK-2j	RISK-2.j	N/A	Threat management information from THREAT domain activities is used to update cyber risks and identify new risks	Functional	Intersects With	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	8	
RISK-2k	RISK-2.k	N/A	Information from THIRD-PARTIES domain activities is used to update cyber risks and identify new risks	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	8	
RISK-2l	RISK-2.l	N/A	Information from ARCHITECTURE domain activities (such as unmitigated architectural conformance gaps) is used to update cyber risks and identify new risks	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.	8	
RISK-2l	RISK-2.l	N/A	Information from ARCHITECTURE domain activities (such as unmitigated architectural conformance gaps) is used to update cyber risks and identify new risks	Functional	Intersects With	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of security, compliance and resilience controls and related processes.	5	
RISK-2l	RISK-2.l	N/A	Information from ARCHITECTURE domain activities (such as unmitigated architectural conformance gaps) is used to update cyber risks and identify new risks	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	8	

FDE #	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-2l	RISK-2.l	N/A	Information from ARCHITECTURE domain activities (such as unmitigated architectural conformance gaps) is used to update cyber risks and identify new risks	Functional	Intersects With	Time To Remediate / Benchmarks For Corrective Action	VPM-05.3	Mechanisms exist to track the effectiveness of remediation operations through metrics reporting.	5	
RISK-2m	RISK-2.m	N/A	Cyber risk identification considers risks that may arise from or impact critical infrastructure or other interdependent organizations	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	
RISK-2m	RISK-2.m	N/A	Cyber risk identification considers risks that may arise from or impact critical infrastructure or other interdependent organizations	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	
RISK-2m	RISK-2.m	N/A	Cyber risk identification considers risks that may arise from or impact critical infrastructure or other interdependent organizations	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify:(1) Assumptions affecting risk assessments, risk response and risk monitoring;(2) Constraints affecting risk assessments, risk response and risk monitoring;(3) The organizational risk tolerance; and(4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
RISK-2m	RISK-2.m	N/A	Cyber risk identification considers risks that may arise from or impact critical infrastructure or other interdependent organizations	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
RISK-3a	RISK-3.a	N/A	Cyber risks are prioritized based on estimated impact, at least in an ad hoc manner	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-3b	RISK-3.b	N/A	Defined criteria are used to prioritize cyber risks (for example, impact to the organization, impact to the community, likelihood, susceptibility, risk tolerance)	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify:(1) Assumptions affecting risk assessments, risk response and risk monitoring;(2) Constraints affecting risk assessments, risk response and risk monitoring;(3) The organizational risk tolerance; and(4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
RISK-3c	RISK-3.c	N/A	A defined method is used to estimate impact for higher priority cyber risks (for example, comparison to actual events, risk quantification)	Functional	Subset Of	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.	10	
RISK-3d	RISK-3.d	N/A	Defined methods are used to analyze higher priority cyber risks (for example, analyzing the prevalence of types of attacks to estimate likelihood, using the results of controls assessments to estimate susceptibility)	Functional	Subset Of	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.	10	
RISK-3e	RISK-3.e	N/A	Organizational stakeholders from appropriate operations and business functions participate in the analysis of higher priority cyber risks	Functional	Subset Of	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.	10	
RISK-3f	RISK-3.f	N/A	Cyber risks are removed from the risk register or other artifact used to document and manage identified risks when they no longer require tracking or response	Functional	Subset Of	Capabilities Deficiency Tracking	IAO-05	minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the	10	
RISK-3f	RISK-3.f	N/A	Cyber risks are removed from the risk register or other artifact used to document and manage identified risks when they no longer require tracking or response	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	8	
RISK-3g	RISK-3.g	N/A	Cyber risk analyses are updated periodically and according to defined triggers, such as system changes, external events, and information from other model domains	Functional	Subset Of	Capabilities Deficiency Tracking	IAO-05	minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the	10	
RISK-4a	RISK-4.a	N/A	Risk responses (such as mitigate, accept, avoid, or transfer) are implemented to address cyber risks, at least in an ad hoc manner	Functional	Intersects With	Risk Treatment Options	RSK-06.3	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings.	5	
RISK-4b	RISK-4.b	N/A	A defined method is used to select and implement risk responses based on analysis and prioritization	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.	8	
RISK-4b	RISK-4.b	N/A	A defined method is used to select and implement risk responses based on analysis and prioritization	Functional	Intersects With	Risk Treatment Options	RSK-06.3	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings.	8	
RISK-4c	RISK-4.c	N/A	Cybersecurity controls are evaluated to determine whether they are designed appropriately and are operating as intended to mitigate identified cyber risks	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.	8	
RISK-4c	RISK-4.c	N/A	Cybersecurity controls are evaluated to determine whether they are designed appropriately and are operating as intended to mitigate identified cyber risks	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	8	
RISK-4c	RISK-4.c	N/A	Cybersecurity controls are evaluated to determine whether they are designed appropriately and are operating as intended to mitigate identified cyber risks	Functional	Intersects With	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	8	
RISK-4c	RISK-4.c	N/A	Cybersecurity controls are evaluated to determine whether they are designed appropriately and are operating as intended to mitigate identified cyber risks	Functional	Intersects With	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	8	
RISK-4d	RISK-4.d	N/A	Results from cyber risk impact analyses and cybersecurity control evaluations are reviewed together by enterprise leadership to determine whether cyber risks are sufficiently mitigated, and risk tolerances are not exceeded	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	8	
RISK-4e	RISK-4.e	N/A	Risk responses (such as mitigate, accept, avoid, or transfer) are reviewed periodically by leadership to determine whether they are still appropriate	Functional	Subset Of	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	10	
RISK-4e	RISK-4.e	N/A	Risk responses (such as mitigate, accept, avoid, or transfer) are reviewed periodically by leadership to determine whether they are still appropriate	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related:(1) Assessments;(2) Audits; and/or(3) Incidents.	8	
RISK-5a	RISK-5.a	N/A	Documented procedures are established, followed, and maintained for activities in the RISK domain	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	
RISK-5b	RISK-5.b	N/A	Adequate resources (people, funding, and tools) are provided to support activities in the RISK domain	Functional	Subset Of	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	
RISK-5c	RISK-5.c	N/A	Up-to-date policies or other organizational directives define requirements for activities in the RISK domain	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
RISK-5d	RISK-5.d	N/A	Responsibility, accountability, and authority for the performance of activities in the RISK domain are assigned to personnel	Functional	Subset Of	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	10	
RISK-5e	RISK-5.e	N/A	Personnel performing activities in the RISK domain have the skills and knowledge needed to perform their assigned responsibilities	Functional	Subset Of	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	10	
RISK-5f	RISK-5.f	N/A	The effectiveness of activities in the RISK domain is evaluated and tracked	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	10	
ACCESS-1a	ACCESS-1.a	N/A	Identities are provisioned, at least in an ad hoc manner, for personnel and other entities such as services and devices that require access to assets (note that this does not preclude shared identities)	Functional	Subset Of	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	10	
ACCESS-1b	ACCESS-1.b	N/A	Credentials (such as passwords, smartcards, certificates, and keys) are issued for personnel and other entities that require access to assets, at least in an ad hoc manner	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	8	
ACCESS-1b	ACCESS-1.b	N/A	Credentials (such as passwords, smartcards, certificates, and keys) are issued for personnel and other entities that require access to assets, at least in an ad hoc manner	Functional	Subset Of	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
ACCESS-1b	ACCESS-1.b	N/A	Credentials (such as passwords, smartcards, certificates, and keys) are issued for personnel and other entities that require access to assets, at least in an ad hoc manner	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	8	
ACCESS-1b	ACCESS-1.b	N/A	Credentials (such as passwords, smartcards, certificates, and keys) are issued for personnel and other entities that require access to assets, at least in an ad hoc manner	Functional	Intersects With	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	8	
ACCESS-1c	ACCESS-1.c	N/A	Identities are deprovisioned, at least in an ad hoc manner, when no longer required	Functional	Subset Of	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	10	
ACCESS-1d	ACCESS-1.d	N/A	Password strength and reuse restrictions are defined and enforced	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	8	
ACCESS-1e	ACCESS-1.e	N/A	Identity repositories are reviewed and updated periodically and according to defined triggers, such as system changes and changes to organizational structure	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	
ACCESS-1f	ACCESS-1.f	N/A	Identities are deprovisioned within organization-defined time thresholds when no longer required	Functional	Subset Of	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	10	
ACCESS-1g	ACCESS-1.g	N/A	The use of privileged credentials is limited to processes for which they are required	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.	8	
ACCESS-1g	ACCESS-1.g	N/A	The use of privileged credentials is limited to processes for which they are required	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8	
ACCESS-1g	ACCESS-1.g	N/A	The use of privileged credentials is limited to processes for which they are required	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	8	
ACCESS-1h	ACCESS-1.h	N/A	Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access)	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:(1) Remote network access;(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or(3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5	
ACCESS-1h	ACCESS-1.h	N/A	Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access)	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
ACCESS-1h	ACCESS-1.h	N/A	Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access)	Functional	Intersects With	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	
ACCESS-1h	ACCESS-1.h	N/A	Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access)	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
ACCESS-1i	ACCESS-1.i	N/A	Multifactor authentication is required for all access, where feasible	Functional	Subset Of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:(1) Remote network access;(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or(3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	10	
ACCESS-1j	ACCESS-1.j	N/A	Identities are disabled after a defined period of inactivity, where feasible	Functional	Equal	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	10	
ACCESS-2a	ACCESS-2.a	N/A	Logical access controls are implemented, at least in an ad hoc manner	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ACCESS-2b	ACCESS-2.b	N/A	Logical access privileges are revoked when no longer needed, at least in an ad hoc manner	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.	8	

FDE #	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
ACCESS-2b	ACCESS-2.b	N/A	Logical access privileges are revoked when no longer needed, at least in an ad hoc manner	Functional	Subset Of	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	10	
ACCESS-2b	ACCESS-2.b	N/A	Logical access privileges are revoked when no longer needed, at least in an ad hoc manner	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
ACCESS-2b	ACCESS-2.b	N/A	Logical access privileges are revoked when no longer needed, at least in an ad hoc manner	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.	8	
ACCESS-2c	ACCESS-2.c	N/A	Logical access requirements are established and maintained (for example, rules for which types of entities are allowed to access an asset, limits of allowed access, constraints on remote access, authentication parameters)	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ACCESS-2d	ACCESS-2.d	N/A	Logical access requirements incorporate the principle of least privilege	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	8	
ACCESS-2d	ACCESS-2.d	N/A	Logical access requirements incorporate the principle of least privilege	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	8	
ACCESS-2e	ACCESS-2.e	N/A	Logical access requirements incorporate the principle of separation of duties	Functional	Subset Of	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	10	
ACCESS-2f	ACCESS-2.f	N/A	Logical access requests are reviewed and approved by the asset owner	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
ACCESS-2f	ACCESS-2.f	N/A	Logical access requests are reviewed and approved by the asset owner	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	8	
ACCESS-2f	ACCESS-2.f	N/A	Logical access requests are reviewed and approved by the asset owner	Functional	Intersects With	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	8	
ACCESS-2f	ACCESS-2.f	N/A	Logical access requests are reviewed and approved by the asset owner	Functional	Intersects With	Management Approval For Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.	8	
ACCESS-2f	ACCESS-2.f	N/A	Logical access requests are reviewed and approved by the asset owner	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	8	
ACCESS-2g	ACCESS-2.g	N/A	Logical access privileges that pose higher risk to the function receive additional scrutiny and monitoring	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	8	
ACCESS-2g	ACCESS-2.g	N/A	Logical access privileges that pose higher risk to the function receive additional scrutiny and monitoring	Functional	Intersects With	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	8	
ACCESS-2g	ACCESS-2.g	N/A	Logical access privileges that pose higher risk to the function receive additional scrutiny and monitoring	Functional	Intersects With	Management Approval For Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.	8	
ACCESS-2g	ACCESS-2.g	N/A	Logical access privileges that pose higher risk to the function receive additional scrutiny and monitoring	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	8	
ACCESS-2h	ACCESS-2.h	N/A	Logical access privileges are reviewed and updated to ensure conformance with access requirements periodically and according to defined triggers, such as changes to organizational structure, and after any temporary elevation of privileges	Functional	Intersects With	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	8	
ACCESS-2h	ACCESS-2.h	N/A	Logical access privileges are reviewed and updated to ensure conformance with access requirements periodically and according to defined triggers, such as changes to organizational structure, and after any temporary elevation of 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.	8	
ACCESS-2i	ACCESS-2.i	N/A	Anomalous logical access attempts are monitored as indicators of cybersecurity events	Functional	Subset Of	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	10	
ACCESS-3a	ACCESS-3.a	N/A	Physical access controls (such as fences, locks, and signage) are implemented, at least in an ad hoc manner	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
ACCESS-3a	ACCESS-3.a	N/A	Physical access controls (such as fences, locks, and signage) are implemented, at least in an ad hoc manner	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	8	
ACCESS-3b	ACCESS-3.b	N/A	Physical access privileges are revoked when no longer needed, at least in an ad hoc manner	Functional	Subset Of	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	
ACCESS-3c	ACCESS-3.c	N/A	Physical access logs are maintained, at least in an ad hoc manner	Functional	Subset Of	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	10	
ACCESS-3d	ACCESS-3.d	N/A	Physical access requirements are established and maintained (for example, rules for who is allowed to access an asset, how access is granted, limits of allowed access)	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
ACCESS-3d	ACCESS-3.d	N/A	Physical access requirements are established and maintained (for example, rules for who is allowed to access an asset, how access is granted, limits of allowed access)	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	8	
ACCESS-3d	ACCESS-3.d	N/A	Physical access requirements are established and maintained (for example, rules for who is allowed to access an asset, how access is granted, limits of allowed access)	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	8	
ACCESS-3e	ACCESS-3.e	N/A	Physical access requirements incorporate the principle of least privilege	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	8	
ACCESS-3e	ACCESS-3.e	N/A	Physical access requirements incorporate the principle of least privilege	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	8	
ACCESS-3f	ACCESS-3.f	N/A	Physical access requirements incorporate the principle of separation of duties	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	8	
ACCESS-3f	ACCESS-3.f	N/A	Physical access requirements incorporate the principle of separation of duties	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	8	
ACCESS-3f	ACCESS-3.f	N/A	Physical access requirements incorporate the principle of separation of duties	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	8	
ACCESS-3f	ACCESS-3.f	N/A	Physical access requirements incorporate the principle of separation of duties	Functional	Intersects With	Dual Authorization for Physical Access	PES-02.2	Mechanisms exist to enforce a "two-person rule" for physical access by requiring two authorized individuals with separate access cards, keys or PINs, to access highly-sensitive areas (e.g., safe, high-security cage, etc.).	3	
ACCESS-3f	ACCESS-3.f	N/A	Physical access requirements incorporate the principle of separation of duties	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
ACCESS-3g	ACCESS-3.g	N/A	Physical access requests are reviewed and approved by the asset owner	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
ACCESS-3g	ACCESS-3.g	N/A	Physical access requests are reviewed and approved by the asset owner	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
ACCESS-3h	ACCESS-3.h	N/A	Physical access privileges that pose higher risk to the function receive additional scrutiny and monitoring	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
ACCESS-3h	ACCESS-3.h	N/A	Physical access privileges that pose higher risk to the function receive additional scrutiny and monitoring	Functional	Intersects With	Users With Elevated Privileges	HRS-02.1	Mechanisms exist to ensure that every user accessing Technology Assets, Applications and/or Services (TAAS) that process, store and/or transmit sensitive/regulated data is cleared and regularly trained to handle the information in question.	5	
ACCESS-3h	ACCESS-3.h	N/A	Physical access privileges that pose higher risk to the function receive additional scrutiny and monitoring	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	8	
ACCESS-3i	ACCESS-3.i	N/A	Physical access privileges are reviewed and updated	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	8	
ACCESS-3j	ACCESS-3.j	N/A	Physical access is monitored to identify potential cybersecurity events	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	8	
ACCESS-4a	ACCESS-4.a	N/A	Documented procedures are established, followed, and maintained for activities in the ACCESS domain	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	
ACCESS-4b	ACCESS-4.b	N/A	Adequate resources (people, funding, and tools) are provided to support activities in the ACCESS domain	Functional	Subset Of	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	
ACCESS-4c	ACCESS-4.c	N/A	Up-to-date policies or other organizational directives define requirements for activities in the ACCESS domain	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
ACCESS-4d	ACCESS-4.d	N/A	Responsibility, accountability, and authority for the performance of activities in the ACCESS domain are assigned to personnel	Functional	Subset Of	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	10	
ACCESS-4e	ACCESS-4.e	N/A	Personnel performing activities in the ACCESS domain have the skills and knowledge needed to perform their assigned responsibilities	Functional	Subset Of	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	10	
ACCESS-4f	ACCESS-4.f	N/A	The effectiveness of activities in the ACCESS domain is evaluated and tracked	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	10	
SITUATION-1a	SITUATION-1.a	N/A	Logging is occurring for assets that are important to the delivery of the function, at least in an ad hoc manner	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
SITUATION-1a	SITUATION-1.a	N/A	Logging is occurring for assets that are important to the delivery of the function, at least in an ad hoc manner	Functional	Intersects With	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.	8	
SITUATION-1a	SITUATION-1.a	N/A	Logging is occurring for assets that are important to the delivery of the function, at least in an ad hoc manner	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	8	
SITUATION-1b	SITUATION-1.b	N/A	Logging is occurring for assets within the function that may be leveraged to achieve a threat objective, wherever feasible	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	
SITUATION-1c	SITUATION-1.c	N/A	Logging requirements are established and maintained for IT and OT assets that are important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
SITUATION-1c	SITUATION-1.c	N/A	Logging requirements are established and maintained for IT and OT assets that are important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective	Functional	Intersects With	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.	8	
SITUATION-1d	SITUATION-1.d	N/A	Logging requirements are established and maintained for network and host monitoring infrastructure (for example, web gateways, endpoint detection and response software, intrusion detection and prevention systems)	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
SITUATION-1d	SITUATION-1.d	N/A	Logging requirements are established and maintained for network and host monitoring infrastructure (for example, web gateways, endpoint detection and response software, intrusion detection and prevention systems)	Functional	Intersects With	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.	8	
SITUATION-1e	SITUATION-1.e	N/A	Log data are being aggregated within the function	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	8	
SITUATION-1e	SITUATION-1.e	N/A	Log data are being aggregated within the function	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	8	

FDE #	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
SITUATION-1f	SITUATION-1.f	N/A	More rigorous logging is performed for higher priority assets	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	8	
SITUATION-1f	SITUATION-1.f	N/A	More rigorous logging is performed for higher priority assets	Functional	Subset Of	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.	10	
SITUATION-1f	SITUATION-1.f	N/A	More rigorous logging is performed for higher priority assets	Functional	Intersects With	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.	5	
SITUATION-1f	SITUATION-1.f	N/A	More rigorous logging is performed for higher priority assets	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	8	
SITUATION-2a	SITUATION-2.a	N/A	Periodic reviews of log data or other cybersecurity monitoring activities are performed, at least in an ad hoc manner	Functional	Subset Of	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	10	
SITUATION-2b	SITUATION-2.b	N/A	Data and alerts from network and host monitoring infrastructure assets are periodically reviewed, at least in an ad hoc manner	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	8	
SITUATION-2b	SITUATION-2.b	N/A	Data and alerts from network and host monitoring infrastructure assets are periodically reviewed, at least in an ad hoc manner	Functional	Subset Of	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	10	
SITUATION-2c	SITUATION-2.c	N/A	Monitoring and analysis requirements are established and maintained for the function and address timely review of event data	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
SITUATION-2d	SITUATION-2.d	N/A	Indicators of anomalous activity are established and maintained based on system logs, data flows, network baselines, cybersecurity events, and architecture and are monitored across the IT and OT environments	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	8	
SITUATION-2d	SITUATION-2.d	N/A	Indicators of anomalous activity are established and maintained based on system logs, data flows, network baselines, cybersecurity events, and architecture and are monitored across the IT and OT environments	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
SITUATION-2d	SITUATION-2.d	N/A	Indicators of anomalous activity are established and maintained based on system logs, data flows, network baselines, cybersecurity events, and architecture and are monitored across the IT and OT environments	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	8	
SITUATION-2e	SITUATION-2.e	N/A	Alarms and alerts are configured and maintained to support the identification of cybersecurity events	Functional	Intersects With	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.	8	
SITUATION-2e	SITUATION-2.e	N/A	Alarms and alerts are configured and maintained to support the identification of cybersecurity events	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	8	
SITUATION-2f	SITUATION-2.f	N/A	Monitoring activities are aligned with the threat profile (THREAT-2e)	Functional	Subset Of	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	10	
SITUATION-2g	SITUATION-2.g	N/A	More rigorous monitoring is performed for higher priority assets	Functional	Subset Of	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	10	
SITUATION-2h	SITUATION-2.h	N/A	Risk analysis information (RISK-3d) is used to identify indicators of anomalous activity	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	8	
SITUATION-2h	SITUATION-2.h	N/A	Risk analysis information (RISK-3d) is used to identify indicators of anomalous activity	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
SITUATION-2h	SITUATION-2.h	N/A	Risk analysis information (RISK-3d) is used to identify indicators of anomalous activity	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	8	
SITUATION-2h	SITUATION-2.h	N/A	Risk analysis information (RISK-3d) is used to identify indicators of anomalous activity	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify:(1) Assumptions affecting risk assessments, risk response and risk monitoring;(2) Constraints affecting risk assessments, risk response and risk monitoring;(3) The organizational risk tolerance; and(4) Priorities, benefits and trade-offs considered by the organization for managing risk.	8	
SITUATION-2i	SITUATION-2.i	N/A	Indicators of anomalous activity are evaluated and updated periodically and according to defined triggers, such as system changes and external events	Functional	Subset Of	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	10	
SITUATION-2i	SITUATION-2.i	N/A	Indicators of anomalous activity are evaluated and updated periodically and according to defined triggers, such as system changes and external events	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	8	
SITUATION-2i	SITUATION-2.i	N/A	Indicators of anomalous activity are evaluated and updated periodically and according to defined triggers, such as system changes and external events	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
SITUATION-2i	SITUATION-2.i	N/A	Indicators of anomalous activity are evaluated and updated periodically and according to defined triggers, such as system changes and external events	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	8	
SITUATION-3a	SITUATION-3.a	N/A	Methods of communicating the current state of cybersecurity for the function are established and maintained	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	8	
SITUATION-3a	SITUATION-3.a	N/A	Methods of communicating the current state of cybersecurity for the function are established and maintained	Functional	Intersects With	Trend Analysis Reporting	MON-06.2	Mechanisms exist to employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.	5	
SITUATION-3b	SITUATION-3.b	N/A	Monitoring data are aggregated to provide an understanding of the operational state of the function	Functional	Subset Of	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	
SITUATION-3c	SITUATION-3.c	N/A	Relevant information from across the organization is available to enhance situational awareness	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	8	
SITUATION-3c	SITUATION-3.c	N/A	Relevant information from across the organization is available to enhance situational awareness	Functional	Intersects With	Trend Analysis Reporting	MON-06.2	Mechanisms exist to employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.	8	
SITUATION-3d	SITUATION-3.d	N/A	Situational awareness reporting requirements have been defined and address timely dissemination of cybersecurity information to organization-defined stakeholders	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	8	
SITUATION-3d	SITUATION-3.d	N/A	Situational awareness reporting requirements have been defined and address timely dissemination of cybersecurity information to organization-defined stakeholders	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	8	
SITUATION-3d	SITUATION-3.d	N/A	Situational awareness reporting requirements have been defined and address timely dissemination of cybersecurity information to organization-defined stakeholders	Functional	Intersects With	Trend Analysis Reporting	MON-06.2	Mechanisms exist to employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.	8	
SITUATION-3e	SITUATION-3.e	N/A	Relevant information from outside the organization is collected and made available across the organization to enhance situational awareness	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	8	
SITUATION-3e	SITUATION-3.e	N/A	Relevant information from outside the organization is collected and made available across the organization to enhance situational awareness	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	8	
SITUATION-3f	SITUATION-3.f	N/A	A capability is established and maintained to aggregate, correlate, and analyze the outputs of cybersecurity monitoring activities and provide a near-real-time understanding of the cybersecurity state of the function	Functional	Subset Of	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	10	
SITUATION-3g	SITUATION-3.g	N/A	Predefined states of operation are documented and can be implemented based on the cybersecurity state of the function or when triggered by activities in other domains	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
SITUATION-3g	SITUATION-3.g	N/A	Predefined states of operation are documented and can be implemented based on the cybersecurity state of the function or when triggered by activities in other domains	Functional	Intersects With	Alert Threshold Tuning	MON-01.13	Mechanisms exist to "tune" event monitoring technologies through analyzing communications traffic/event patterns and developing profiles representing common traffic patterns and/or events.	5	
SITUATION-3g	SITUATION-3.g	N/A	Predefined states of operation are documented and can be implemented based on the cybersecurity state of the function or when triggered by activities in other domains	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	5	
SITUATION-4a	SITUATION-4.a	N/A	Documented procedures are established, followed, and maintained for activities in the SITUATION domain	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	
SITUATION-4b	SITUATION-4.b	N/A	Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	Functional	Subset Of	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	
SITUATION-4c	SITUATION-4.c	N/A	Up-to-date policies or other organizational directives define requirements for activities in the SITUATION domain	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
SITUATION-4d	SITUATION-4.d	N/A	Responsibility, accountability, and authority for the performance of activities in the SITUATION domain are assigned to personnel	Functional	Subset Of	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	10	
SITUATION-4e	SITUATION-4.e	N/A	Personnel performing activities in the SITUATION domain have the skills and knowledge needed to perform their assigned responsibilities	Functional	Subset Of	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	10	
SITUATION-4f	SITUATION-4.f	N/A	The effectiveness of activities in the SITUATION domain is evaluated and tracked	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	10	
RESPONSE-1a	RESPONSE-1.a	N/A	Detected cybersecurity events are reported to a specified person or role and documented, at least in an ad hoc manner	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	
RESPONSE-1a	RESPONSE-1.a	N/A	Detected cybersecurity events are reported to a specified person or role and documented, at least in an ad hoc manner	Functional	Intersects With	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.	8	
RESPONSE-1a	RESPONSE-1.a	N/A	Detected cybersecurity events are reported to a specified person or role and documented, at least in an ad hoc manner	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	
RESPONSE-1b	RESPONSE-1.b	N/A	Criteria are established for cybersecurity event detection (for example, what constitutes a cybersecurity event, where to look for cybersecurity events)	Functional	Intersects With	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.	5	
RESPONSE-1b	RESPONSE-1.b	N/A	Criteria are established for cybersecurity event detection (for example, what constitutes a cybersecurity event, where to look for cybersecurity events)	Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	8	
RESPONSE-1c	RESPONSE-1.c	N/A	Cybersecurity events are documented based on the established criteria	Functional	Subset Of	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	10	
RESPONSE-1d	RESPONSE-1.d	N/A	Event information is correlated to support incident analysis by identifying patterns, trends, and other common features	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
RESPONSE-1d	RESPONSE-1.d	N/A	Event information is correlated to support incident analysis by identifying patterns, trends, and other common features	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	

FDE #	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
RESPONSE-1d	RESPONSE-1.d	N/A	Event information is correlated to support incident analysis by identifying patterns, trends, and other common features	Functional	Intersects With	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.	5	
RESPONSE-1e	RESPONSE-1.e	N/A	Cybersecurity event detection activities are adjusted based on identified risks and the organization's threat profile (THREAT-2e)	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	8	
RESPONSE-1f	RESPONSE-1.f	N/A	Situational awareness for the function is monitored to support the identification of cybersecurity events	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	
RESPONSE-2a	RESPONSE-2.a	N/A	Criteria for declaring cybersecurity incidents are established, at least in an ad hoc manner	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	
RESPONSE-2a	RESPONSE-2.a	N/A	Criteria for declaring cybersecurity incidents are established, at least in an ad hoc manner	Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	8	
RESPONSE-2b	RESPONSE-2.b	N/A	Cybersecurity events are analyzed to support the declaration of cybersecurity incidents, at least in an ad hoc manner	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	
RESPONSE-2b	RESPONSE-2.b	N/A	Cybersecurity events are analyzed to support the declaration of cybersecurity incidents, at least in an ad hoc manner	Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	8	
RESPONSE-2c	RESPONSE-2.c	N/A	Cybersecurity incident declaration criteria are formally established based on potential impact to the function	Functional	Subset Of	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	10	
RESPONSE-2d	RESPONSE-2.d	N/A	Cybersecurity events are declared to be incidents based on established criteria	Functional	Subset Of	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	10	
RESPONSE-2e	RESPONSE-2.e	N/A	Cybersecurity incident declaration criteria are updated periodically and according to defined triggers, such as organizational changes, lessons learned from plan execution, or newly identified threats	Functional	Subset Of	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	10	
RESPONSE-2f	RESPONSE-2.f	N/A	There is a repository where cybersecurity events and incidents are documented and tracked to closure	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	8	
RESPONSE-2f	RESPONSE-2.f	N/A	There is a repository where cybersecurity events and incidents are documented and tracked to closure	Functional	Subset Of	Incident Tracking Repository	IRO-09.3	incidents document:(1) Details of the incident (e.g., category, severity, affected parties, etc.);(2) Remediation actions taken through incident	10	
RESPONSE-2g	RESPONSE-2.g	N/A	Internal and external stakeholders (for example, executives, attorneys, government agencies, connected organizations, vendors, sector organizations, regulators) are identified and notified of incidents based on situational awareness reporting requirements (SITUATION-3d)	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
RESPONSE-2g	RESPONSE-2.g	N/A	Internal and external stakeholders (for example, executives, attorneys, government agencies, connected organizations, vendors, sector organizations, regulators) are identified and notified of incidents based on situational awareness reporting requirements (SITUATION-3d)	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
RESPONSE-2h	RESPONSE-2.h	N/A	Criteria for cybersecurity incident declaration are aligned with cyber risk prioritization criteria (RISK-3b)	Functional	Subset Of	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	10	
RESPONSE-2i	RESPONSE-2.i	N/A	Cybersecurity incidents are correlated to identify patterns, trends, and other common features across multiple incidents	Functional	Subset Of	Incident Pattern Analysis	IRO-09.4	Mechanisms exist to analyze historical incidents in aggregate to identify:(1) Patterns;(2) Trends; and(3) Other common root causes in order to address the vulnerability and risk	10	
RESPONSE-3a	RESPONSE-3.a	N/A	Cybersecurity incident response personnel are identified, and roles are assigned, at least in an ad hoc manner	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
RESPONSE-3a	RESPONSE-3.a	N/A	Cybersecurity incident response personnel are identified, and roles are assigned, at least in an ad hoc manner	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	8	
RESPONSE-3b	RESPONSE-3.b	N/A	Responses to cybersecurity incidents are executed, at least in an ad hoc manner, to limit impact to the function and restore normal operations	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	
RESPONSE-3b	RESPONSE-3.b	N/A	Responses to cybersecurity incidents are executed, at least in an ad hoc manner, to limit impact to the function and restore normal operations	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	
RESPONSE-3c	RESPONSE-3.c	N/A	Reporting of incidents is performed (for example, internal reporting, ICS-CERT, relevant ISACs), at least in an ad hoc manner	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	
RESPONSE-3c	RESPONSE-3.c	N/A	Reporting of incidents is performed (for example, internal reporting, ICS-CERT, relevant ISACs), at least in an ad hoc manner	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	8	
RESPONSE-3c	RESPONSE-3.c	N/A	Reporting of incidents is performed (for example, internal reporting, ICS-CERT, relevant ISACs), at least in an ad hoc manner	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
RESPONSE-3d	RESPONSE-3.d	N/A	Cybersecurity incident response plans that address all phases of the incident lifecycle are established and maintained	Functional	Subset Of	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	
RESPONSE-3e	RESPONSE-3.e	N/A	Cybersecurity incident response is executed according to defined plans and procedures	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	
RESPONSE-3e	RESPONSE-3.e	N/A	Cybersecurity incident response is executed according to defined plans and procedures	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	
RESPONSE-3f	RESPONSE-3.f	N/A	Cybersecurity incident response plans include a communications plan for internal and external stakeholders	Functional	Subset Of	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	
RESPONSE-3g	RESPONSE-3.g	N/A	Cybersecurity incident response plan exercises are conducted periodically and according to defined triggers, such as system changes and external events	Functional	Subset Of	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	10	
RESPONSE-3h	RESPONSE-3.h	N/A	Cybersecurity incident lessons-learned activities are performed and corrective actions are taken, including updates to the incident response plan	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	
RESPONSE-3i	RESPONSE-3.i	N/A	Cybersecurity incident root-cause analysis is performed and corrective actions are taken, including updates to the incident response plan	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	
RESPONSE-3j	RESPONSE-3.j	N/A	Cybersecurity incident responses are coordinated with vendors, law enforcement, and other external entities as appropriate, including support for evidence collection and preservation	Functional	Subset Of	Coordination with Related Plans	IRO-06.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.	10	
RESPONSE-3j	RESPONSE-3.j	N/A	Cybersecurity incident responses are coordinated with vendors, law enforcement, and other external entities as appropriate, including support for evidence collection and preservation	Functional	Intersects With	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	8	
RESPONSE-3k	RESPONSE-3.k	N/A	Cybersecurity incident response personnel participate in joint cybersecurity exercises with other organizations	Functional	Intersects With	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	8	
RESPONSE-3l	RESPONSE-3.l	N/A	Cybersecurity incident responses leverage and trigger predefined states of operation (SITUATION-3g)	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	
RESPONSE-3l	RESPONSE-3.l	N/A	Cybersecurity incident responses leverage and trigger predefined states of operation (SITUATION-3g)	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	
RESPONSE-4a	RESPONSE-4.a	N/A	Continuity plans are developed to sustain and restore operation of the function if a cybersecurity event or incident occurs, at least in an ad hoc manner	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	
RESPONSE-4b	RESPONSE-4.b	N/A	Data backups are available and tested, at least in an ad hoc manner	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8	
RESPONSE-4b	RESPONSE-4.b	N/A	Data backups are available and tested, at least in an ad hoc manner	Functional	Intersects With	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	8	
RESPONSE-4c	RESPONSE-4.c	N/A	IT and OT assets requiring spares are identified, at least in an ad hoc manner	Functional	Subset Of	Reserve Hardware	BCD-15	Mechanisms exist to purchase and maintain a sufficient reserve of spare hardware to ensure essential missions and business functions can be maintained in the event of a supply chain disruption.	10	
RESPONSE-4d	RESPONSE-4.d	N/A	Continuity plans address potential impacts from cybersecurity incidents	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	
RESPONSE-4e	RESPONSE-4.e	N/A	The assets and activities necessary to sustain minimum operations of the function are identified and documented in continuity plans	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	
RESPONSE-4f	RESPONSE-4.f	N/A	Continuity plans address IT, OT, and information assets that are important to the delivery of the function, including the availability of backup data and replacement, redundant, and spare IT and OT assets	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	
RESPONSE-4g	RESPONSE-4.g	N/A	Recovery time objectives (RTOs) and recovery point objectives (RPOs) for assets that are important to the delivery of the function are incorporated into continuity plans	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8	
RESPONSE-4g	RESPONSE-4.g	N/A	Recovery time objectives (RTOs) and recovery point objectives (RPOs) for assets that are important to the delivery of the function are incorporated into continuity plans	Functional	Intersects With	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.	8	
RESPONSE-4h	RESPONSE-4.h	N/A	Cybersecurity incident criteria that trigger the execution of continuity plans are established and communicated to incident response and continuity management personnel	Functional	Subset Of	Recovery Operations Criteria	BCD-01.5	Mechanisms exist to define specific criteria that must be met to initiate Business Continuity / Disaster Recover (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	10	
RESPONSE-4i	RESPONSE-4.i	N/A	Continuity plans are tested through evaluations and exercises periodically and according to defined triggers, such as system changes and external events	Functional	Subset Of	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	10	
RESPONSE-4j	RESPONSE-4.j	N/A	Cybersecurity controls protecting backup data are equivalent to or more rigorous than controls protecting source data	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
RESPONSE-4j	RESPONSE-4.j	N/A	Cybersecurity controls protecting backup data are equivalent to or more rigorous than controls protecting source data	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	8	

FDE #	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
RESPONSE-4j	RESPONSE-4.j	N/A	Cybersecurity controls protecting backup data are equivalent to or more rigorous than controls protecting source data	Functional	Intersects With	Backup Access	BCD-11.9	Mechanisms exist to restrict access to backups to privileged users with assigned roles for data backup and recovery operations.	8	
RESPONSE-4k	RESPONSE-4.k	N/A	Data backups are logically or physically separated from source data	Functional	Intersects With	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	5	
RESPONSE-4l	RESPONSE-4.l	N/A	Spares for selected IT and OT assets are available	Functional	Subset Of	Reserve Hardware	BCD-15	Mechanisms exist to purchase and maintain a sufficient reserve of spare hardware to ensure essential missions and business functions can be maintained in the event of a supply chain disruption.	10	
RESPONSE-4m	RESPONSE-4.m	N/A	Continuity plans are aligned with identified risks and the organization's threat profile (THREAT-2e) to ensure coverage of identified risk categories and threats	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	
RESPONSE-4n	RESPONSE-4.n	N/A	Continuity plan exercises address higher priority risks	Functional	Subset Of	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	10	
RESPONSE-4o	RESPONSE-4.o	N/A	The results of continuity plan testing or activation are compared to recovery objectives, and plans are improved accordingly	Functional	Subset Of	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	10	
RESPONSE-4p	RESPONSE-4.p	N/A	Continuity plans are periodically reviewed and updated	Functional	Subset Of	Ongoing Contingency Planning	BCD-06	Mechanisms exist to update contingency plans due to changes affecting:(1) People (e.g., personnel changes);(2) Processes (e.g., new, altered or decommissioned business practices, including third-party services);(3) Technologies (e.g., new, altered or decommissioned technologies);(4) Data (e.g., changes to data flows and/or data repositories);(5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or(6) Feedback from contingency plan testing activities.	10	
RESPONSE-5a	RESPONSE-5.a	N/A	Documented procedures are established, followed, and maintained for activities in the RESPONSE domain	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	
RESPONSE-5b	RESPONSE-5.b	N/A	Adequate resources (people, funding, and tools) are provided to support activities in the RESPONSE domain	Functional	Subset Of	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	
RESPONSE-5c	RESPONSE-5.c	N/A	Up-to-date policies or other organizational directives define requirements for activities in the RESPONSE domain	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
RESPONSE-5d	RESPONSE-5.d	N/A	Responsibility, accountability, and authority for the performance of activities in the RESPONSE domain are assigned to personnel	Functional	Subset Of	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	10	
RESPONSE-5e	RESPONSE-5.e	N/A	Personnel performing activities in the RESPONSE domain have the skills and knowledge needed to perform their assigned responsibilities	Functional	Subset Of	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	10	
RESPONSE-5f	RESPONSE-5.f	N/A	The effectiveness of activities in the RESPONSE domain is evaluated and tracked	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	10	
THIRD-PARTIES-1a	THIRD-PARTIES-1.a	N/A	Important IT and OT third-party dependencies are identified (that is, internal and external parties on which the delivery of the function depends, including operating partners), at least in an ad hoc manner	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	
THIRD-PARTIES-1a	THIRD-PARTIES-1.a	N/A	Important IT and OT third-party dependencies are identified (that is, internal and external parties on which the delivery of the function depends, including operating partners), at least in an ad hoc manner	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	
THIRD-PARTIES-1a	THIRD-PARTIES-1.a	N/A	Important IT and OT third-party dependencies are identified (that is, internal and external parties on which the delivery of the function depends, including operating partners), at least in an ad hoc manner	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	
THIRD-PARTIES-1a	THIRD-PARTIES-1.a	N/A	Important IT and OT third-party dependencies are identified (that is, internal and external parties on which the delivery of the function depends, including operating partners), at least in an ad hoc manner	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	
THIRD-PARTIES-1b	THIRD-PARTIES-1.b	N/A	Third parties that have access to, control of, or custody of any IT, OT, or information assets that are important to the delivery of the function are identified, at least in an ad hoc manner	Functional	Subset Of	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).	10	
THIRD-PARTIES-1c	THIRD-PARTIES-1.c	N/A	A defined method is followed to identify risks arising from suppliers and other third parties	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.	8	
THIRD-PARTIES-1c	THIRD-PARTIES-1.c	N/A	A defined method is followed to identify risks arising from suppliers and other third parties	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).	8	
THIRD-PARTIES-1d	THIRD-PARTIES-1.d	N/A	Third parties are prioritized according to established criteria (for example, importance to the delivery of the function, impact of a compromise or disruption, ability to negotiate cybersecurity requirements within contracts)	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	
THIRD-PARTIES-1d	THIRD-PARTIES-1.d	N/A	Third parties are prioritized according to established criteria (for example, importance to the delivery of the function, impact of a compromise or disruption, ability to negotiate cybersecurity requirements within contracts)	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	
THIRD-PARTIES-1e	THIRD-PARTIES-1.e	N/A	Escalated prioritization is assigned to suppliers and other third parties whose compromise or disruption could cause significant consequences (for example, single-source suppliers, suppliers with privileged access)	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	
THIRD-PARTIES-1f	THIRD-PARTIES-1.f	N/A	Prioritization of suppliers and other third parties is updated periodically and according to defined triggers, such as system changes and external events	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	
THIRD-PARTIES-2a	THIRD-PARTIES-2.a	N/A	The selection of suppliers and other third parties includes consideration of their cybersecurity qualifications, at least in an ad hoc manner	Functional	Subset Of	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).	10	
THIRD-PARTIES-2b	THIRD-PARTIES-2.b	N/A	The selection of products and services includes consideration of their cybersecurity capabilities, at least in an ad hoc manner	Functional	Subset Of	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).	10	
THIRD-PARTIES-2c	THIRD-PARTIES-2.c	N/A	A defined method is followed to identify cybersecurity requirements and implement associated controls that protect against the risks arising from suppliers and other third parties	Functional	Subset Of	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).	10	
THIRD-PARTIES-2d	THIRD-PARTIES-2.d	N/A	A defined method is followed to evaluate and select suppliers and other third parties	Functional	Intersects With	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure security, compliance and resilience control assignments accurately reflect current:(1) Contractual obligations for the External Service Provider (ESP);(2) Business practices;(3) Applicable stakeholders; and(4) Deployed Technology Assets, Applications and/or Services (TAAS).	5	
THIRD-PARTIES-2d	THIRD-PARTIES-2.d	N/A	A defined method is followed to evaluate and select suppliers and other third parties	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	
THIRD-PARTIES-2e	THIRD-PARTIES-2.e	N/A	More rigorous cybersecurity controls are implemented for higher priority suppliers and other third parties	Functional	Subset Of	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).	10	
THIRD-PARTIES-2f	THIRD-PARTIES-2.f	N/A	Cybersecurity requirements (for example, vulnerability notification, incident-related SLA requirements) are formalized in agreements with suppliers and other third parties	Functional	Subset Of	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).	10	
THIRD-PARTIES-2g	THIRD-PARTIES-2.g	N/A	Suppliers and other third parties periodically attest to their ability to meet cybersecurity requirements	Functional	Subset Of	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).	10	
THIRD-PARTIES-2h	THIRD-PARTIES-2.h	N/A	Cybersecurity requirements for suppliers and other third parties include secure software and secure product development requirements where appropriate	Functional	Subset Of	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).	10	
THIRD-PARTIES-2i	THIRD-PARTIES-2.i	N/A	Selection criteria for products include consideration of end-of-life and end-of-support timelines	Functional	Subset Of	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).	10	
THIRD-PARTIES-2i	THIRD-PARTIES-2.i	N/A	Selection criteria for products include consideration of end-of-life and end-of-support timelines	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by:(1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and(2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5	
THIRD-PARTIES-2i	THIRD-PARTIES-2.i	N/A	Selection criteria for products include consideration of end-of-life and end-of-support timelines	Functional	Intersects With	Alternate Sources for Continued Support	TDA-17.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported Technology Assets, Applications and/or Services (TAAS).	5	
THIRD-PARTIES-2j	THIRD-PARTIES-2.j	N/A	Selection criteria include consideration of safeguards against counterfeit or compromised software, hardware, and services	Functional	Subset Of	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	10	
THIRD-PARTIES-2k	THIRD-PARTIES-2.k	N/A	Selection criteria for higher priority assets include evaluation of bills of material for key asset elements, such as hardware and software	Functional	Subset Of	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	10	
THIRD-PARTIES-2l	THIRD-PARTIES-2.l	N/A	Selection criteria for higher priority assets include evaluation of any associated third-party hosting environments and source data	Functional	Subset Of	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	10	
THIRD-PARTIES-2m	THIRD-PARTIES-2.m	N/A	Acceptance testing of procured assets includes consideration of cybersecurity requirements	Functional	Subset Of	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	10	
THIRD-PARTIES-3a	THIRD-PARTIES-3.a	N/A	Documented procedures are established, followed, and maintained for activities in the THIRD-PARTIES domain	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	
THIRD-PARTIES-3b	THIRD-PARTIES-3.b	N/A	Adequate resources (people, funding, and tools) are provided to support activities in the THIRD-PARTIES domain	Functional	Subset Of	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	
THIRD-PARTIES-3c	THIRD-PARTIES-3.c	N/A	Up-to-date policies or other organizational directives define requirements for activities in the THIRD-PARTIES domain	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
THIRD-PARTIES-3d	THIRD-PARTIES-3.d	N/A	Responsibility, accountability, and authority for the performance of activities in the THIRD-PARTIES domain are assigned to personnel	Functional	Subset Of	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	10	
THIRD-PARTIES-3e	THIRD-PARTIES-3.e	N/A	Personnel performing activities in the THIRD-PARTIES domain have the skills and knowledge needed to perform their assigned responsibilities	Functional	Subset Of	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	10	
THIRD-PARTIES-3f	THIRD-PARTIES-3.f	N/A	The effectiveness of activities in the THIRD-PARTIES domain is evaluated and tracked	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	10	
WORKFORCE-1a	WORKFORCE-1.a	N/A	Personnel vetting (for example, background checks, drug tests) is performed at hire, at least in an ad hoc manner	Functional	Subset Of	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	

FDE #	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
WORKFORCE-1b	WORKFORCE-1.b	N/A	Personnel separation procedures address cybersecurity, at least in an ad hoc manner	Functional	Subset Of	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	
WORKFORCE-1c	WORKFORCE-1.c	N/A	Personnel vetting is performed at hire and periodically for positions that have access to assets that are important to the delivery of the function	Functional	Subset Of	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	
WORKFORCE-1d	WORKFORCE-1.d	N/A	Personnel separation and transfer procedures address cybersecurity, including supplementary vetting as appropriate	Functional	Intersects With	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.	8	
WORKFORCE-1d	WORKFORCE-1.d	N/A	Personnel separation and transfer procedures address cybersecurity, including supplementary vetting as appropriate	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	8	
WORKFORCE-1e	WORKFORCE-1.e	N/A	Personnel are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets	Functional	Intersects With	Formal Indoctrination	HRS-04.2	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.	8	
WORKFORCE-1e	WORKFORCE-1.e	N/A	Personnel are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets	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.	8	
WORKFORCE-1e	WORKFORCE-1.e	N/A	Personnel are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	8	
WORKFORCE-1e	WORKFORCE-1.e	N/A	Personnel are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	8	
WORKFORCE-1e	WORKFORCE-1.e	N/A	Personnel are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	8	
WORKFORCE-1e	WORKFORCE-1.e	N/A	Personnel are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	
WORKFORCE-1e	WORKFORCE-1.e	N/A	Personnel are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets	Functional	Intersects With	Use of Critical Technologies	HRS-05.4	Mechanisms exist to govern usage policies for critical technologies.	8	
WORKFORCE-1e	WORKFORCE-1.e	N/A	Personnel are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	8	
WORKFORCE-1e	WORKFORCE-1.e	N/A	Personnel are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets	Functional	Intersects With	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.	8	
WORKFORCE-1e	WORKFORCE-1.e	N/A	Personnel are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	8	
WORKFORCE-1f	WORKFORCE-1.f	N/A	Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
WORKFORCE-1f	WORKFORCE-1.f	N/A	Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	
WORKFORCE-1f	WORKFORCE-1.f	N/A	Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk	Functional	Intersects With	Identity Proofing (Identity Verification)	IAC-28	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.	5	
WORKFORCE-1g	WORKFORCE-1.g	N/A	A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
WORKFORCE-1g	WORKFORCE-1.g	N/A	A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures	Functional	Intersects With	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	8	
WORKFORCE-1g	WORKFORCE-1.g	N/A	A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures	Functional	Intersects With	Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.	8	
WORKFORCE-1g	WORKFORCE-1.g	N/A	A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
WORKFORCE-2a	WORKFORCE-2.a	N/A	Cybersecurity awareness activities occur, at least in an ad hoc manner	Functional	Subset Of	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	10	
WORKFORCE-2a	WORKFORCE-2.a	N/A	Cybersecurity awareness activities occur, at least in an ad hoc manner	Functional	Intersects With	Formal Indoctrination	HRS-04.2	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.	8	
WORKFORCE-2a	WORKFORCE-2.a	N/A	Cybersecurity awareness activities occur, at least in an ad hoc manner	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	8	
WORKFORCE-2a	WORKFORCE-2.a	N/A	Cybersecurity awareness activities occur, at least in an ad hoc manner	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	8	
WORKFORCE-2b	WORKFORCE-2.b	N/A	Cybersecurity awareness objectives 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	
WORKFORCE-2b	WORKFORCE-2.b	N/A	Cybersecurity awareness objectives are established and maintained	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	8	
WORKFORCE-2c	WORKFORCE-2.c	N/A	Cybersecurity awareness objectives are aligned with the defined threat profile (THREAT-2e)	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
WORKFORCE-2c	WORKFORCE-2.c	N/A	Cybersecurity awareness objectives are aligned with the defined threat profile (THREAT-2e)	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	8	
WORKFORCE-2d	WORKFORCE-2.d	N/A	Cybersecurity awareness activities are conducted periodically	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
WORKFORCE-2e	WORKFORCE-2.e	N/A	Cybersecurity awareness activities are tailored to job role	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	
WORKFORCE-2f	WORKFORCE-2.f	N/A	Cybersecurity awareness activities address predefined states of operation (SITUATION-3g)	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	
WORKFORCE-2g	WORKFORCE-2.g	N/A	The effectiveness of cybersecurity awareness activities is evaluated periodically and according to defined triggers, such as system changes and external events, and improvements are made as appropriate	Functional	Subset Of	Maintaining Workforce Development Relevancy	SAT-01.1	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to:(1) Organizational policies, standards and procedures;(2) Assigned roles and responsibilities;(3) Relevant threats and risks; and(4) Technological developments.	10	
WORKFORCE-3a	WORKFORCE-3.a	N/A	Cybersecurity responsibilities for the function are identified, at least in an ad hoc manner	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
WORKFORCE-3a	WORKFORCE-3.a	N/A	Cybersecurity responsibilities for the function are identified, at least in an ad hoc manner	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
WORKFORCE-3b	WORKFORCE-3.b	N/A	Cybersecurity responsibilities are assigned to specific people, at least in an ad hoc manner	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
WORKFORCE-3c	WORKFORCE-3.c	N/A	Cybersecurity responsibilities are assigned to specific roles, including external service providers	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
WORKFORCE-3d	WORKFORCE-3.d	N/A	Cybersecurity responsibilities are documented	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
WORKFORCE-3e	WORKFORCE-3.e	N/A	Cybersecurity responsibilities and job requirements are reviewed and updated periodically and according to defined triggers, such as system changes and changes to organizational structure	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
WORKFORCE-3f	WORKFORCE-3.f	N/A	Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage, including succession planning	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
WORKFORCE-4a	WORKFORCE-4.a	N/A	Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities, at least in an ad hoc manner	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	
WORKFORCE-4b	WORKFORCE-4.b	N/A	Cybersecurity knowledge, skill, and ability requirements and gaps are identified for both current and future operational needs, at least in an ad hoc manner	Functional	Subset Of	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.	10	
WORKFORCE-4c	WORKFORCE-4.c	N/A	Identified cybersecurity knowledge, skill, and ability gaps are addressed through training, recruiting, and retention efforts	Functional	Subset Of	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.	10	
WORKFORCE-4d	WORKFORCE-4.d	N/A	Cybersecurity training is provided as a prerequisite to granting access to assets that are important to the delivery of the function	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	8	
WORKFORCE-4e	WORKFORCE-4.e	N/A	The effectiveness of training programs is evaluated periodically, and improvements are made as appropriate	Functional	Intersects With	Maintaining Workforce Development Relevancy	SAT-01.1	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to:(1) Organizational policies, standards and procedures;(2) Assigned roles and responsibilities;(3) Relevant threats and risks; and(4) Technological developments.	5	
WORKFORCE-4f	WORKFORCE-4.f	N/A	Training programs include continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
WORKFORCE-5a	WORKFORCE-5.a	N/A	Documented procedures are established, followed, and maintained for activities in the WORKFORCE domain	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	
WORKFORCE-5b	WORKFORCE-5.b	N/A	Adequate resources (people, funding, and tools) are provided to support activities in the WORKFORCE domain	Functional	Subset Of	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	
WORKFORCE-5c	WORKFORCE-5.c	N/A	Up-to-date policies or other organizational directives define requirements for activities in the WORKFORCE domain	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
WORKFORCE-5d	WORKFORCE-5.d	N/A	Responsibility, accountability, and authority for the performance of activities in the WORKFORCE domain are assigned to personnel	Functional	Subset Of	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	10	
WORKFORCE-5e	WORKFORCE-5.e	N/A	Personnel performing activities in the WORKFORCE domain have the skills and knowledge needed to perform their assigned responsibilities	Functional	Subset Of	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	10	
WORKFORCE-5f	WORKFORCE-5.f	N/A	The effectiveness of activities in the WORKFORCE domain is evaluated and tracked	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	10	
ARCHITECTURE-1a	ARCHITECTURE-1.a	N/A	The organization has a strategy for cybersecurity architecture, which may be developed and managed in an ad hoc manner	Functional	Subset Of	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.	10	
ARCHITECTURE-1b	ARCHITECTURE-1.b	N/A	A strategy for cybersecurity architecture is established and maintained in alignment with the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture	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	
ARCHITECTURE-1b	ARCHITECTURE-1.b	N/A	A strategy for cybersecurity architecture is established and maintained in alignment with the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
ARCHITECTURE-1b	ARCHITECTURE-1.b	N/A	A strategy for cybersecurity architecture is established and maintained in alignment with the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	

FDE #	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
ARCHITECTURE-1c	ARCHITECTURE-1.c	N/A	A documented cybersecurity architecture is established and maintained that includes IT and OT systems and networks and aligns with system and asset categorization and prioritization	Functional	Subset Of	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	10	
ARCHITECTURE-1d	ARCHITECTURE-1.d	N/A	Governance for cybersecurity architecture (such as an architecture review process) is established and maintained that includes provisions for periodic architectural reviews and an exceptions process	Functional	Subset Of	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	10	
ARCHITECTURE-1e	ARCHITECTURE-1.e	N/A	Senior management sponsorship for the cybersecurity architecture program is visible and active	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	
ARCHITECTURE-1f	ARCHITECTURE-1.f	N/A	The cybersecurity architecture establishes and maintains cybersecurity requirements for the organization's assets	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
ARCHITECTURE-1f	ARCHITECTURE-1.f	N/A	The cybersecurity architecture establishes and maintains cybersecurity requirements for the organization's assets	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.	8	
ARCHITECTURE-1f	ARCHITECTURE-1.f	N/A	The cybersecurity architecture establishes and maintains cybersecurity requirements for the organization's assets	Functional	Subset Of	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of security, compliance and resilience controls and related processes.	10	
ARCHITECTURE-1g	ARCHITECTURE-1.g	N/A	Cybersecurity controls are selected and implemented to meet cybersecurity requirements	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	
ARCHITECTURE-1h	ARCHITECTURE-1.h	N/A	The cybersecurity architecture strategy and program are aligned with the organization's enterprise architecture strategy and program	Functional	Subset Of	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	10	
ARCHITECTURE-1i	ARCHITECTURE-1.i	N/A	Conformance of the organization's systems and networks to the cybersecurity architecture is evaluated periodically and according to defined triggers, such as system changes and external events	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	
ARCHITECTURE-1i	ARCHITECTURE-1.i	N/A	Conformance of the organization's systems and networks to the cybersecurity architecture is evaluated periodically and according to defined triggers, such as system changes and external events	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.	8	
ARCHITECTURE-1i	ARCHITECTURE-1.i	N/A	Conformance of the organization's systems and networks to the cybersecurity architecture is evaluated periodically and according to defined triggers, such as system changes and external events	Functional	Intersects With	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	8	
ARCHITECTURE-1i	ARCHITECTURE-1.i	N/A	Conformance of the organization's systems and networks to the cybersecurity architecture is evaluated periodically and according to defined triggers, such as system changes and external events	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	
ARCHITECTURE-1i	ARCHITECTURE-1.i	N/A	Conformance of the organization's systems and networks to the cybersecurity architecture is evaluated periodically and according to defined triggers, such as system changes and external events	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
ARCHITECTURE-1j	ARCHITECTURE-1.j	N/A	The cybersecurity architecture is guided by the organization's risk analysis information (RISK-3d) and threat profile (THREAT-2e)	Functional	Intersects With	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).	8	
ARCHITECTURE-1j	ARCHITECTURE-1.j	N/A	The cybersecurity architecture is guided by the organization's risk analysis information (RISK-3d) and threat profile (THREAT-2e)	Functional	Intersects With	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
ARCHITECTURE-1j	ARCHITECTURE-1.j	N/A	The cybersecurity architecture is guided by the organization's risk analysis information (RISK-3d) and threat profile (THREAT-2e)	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	
ARCHITECTURE-1j	ARCHITECTURE-1.j	N/A	The cybersecurity architecture is guided by the organization's risk analysis information (RISK-3d) and threat profile (THREAT-2e)	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
ARCHITECTURE-1k	ARCHITECTURE-1.k	N/A	The cybersecurity architecture addresses predefined states of operation (SITUATION-3g)	Functional	Subset Of	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	10	
ARCHITECTURE-2a	ARCHITECTURE-2.a	N/A	Network protections are implemented, at least in an ad hoc manner	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
ARCHITECTURE-2b	ARCHITECTURE-2.b	N/A	The organization's IT systems are separated from OT systems through segmentation, either through physical means or logical means, at least in an ad hoc manner	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	8	
ARCHITECTURE-2c	ARCHITECTURE-2.c	N/A	Network protections are defined and enforced for selected asset types according to asset risk and priority (for example, internal assets, perimeter assets, assets connected to the organization's Wi-Fi, cloud assets, remote access, and externally owned devices)	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
ARCHITECTURE-2c	ARCHITECTURE-2.c	N/A	Network protections are defined and enforced for selected asset types according to asset risk and priority (for example, internal assets, perimeter assets, assets connected to the organization's Wi-Fi, cloud assets, remote access, and externally owned devices)	Functional	Intersects With	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	8	
ARCHITECTURE-2d	ARCHITECTURE-2.d	N/A	Assets that are important to the delivery of the function are logically or physically segmented into distinct security zones based on asset cybersecurity requirements	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	8	
ARCHITECTURE-2e	ARCHITECTURE-2.e	N/A	Network protections incorporate the principles of least privilege and least functionality	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
ARCHITECTURE-2e	ARCHITECTURE-2.e	N/A	Network protections incorporate the principles of least privilege and least functionality	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	8	
ARCHITECTURE-2e	ARCHITECTURE-2.e	N/A	Network protections incorporate the principles of least privilege and least functionality	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	8	
ARCHITECTURE-2f	ARCHITECTURE-2.f	N/A	Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, allowlisting, intrusion detection and prevention systems (IDPS))	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
ARCHITECTURE-2g	ARCHITECTURE-2.g	N/A	Web traffic and email are monitored, analyzed, and controlled (for example, malicious link blocking, suspicious download blocking, email authentication techniques, IP address blocking)	Functional	Subset Of	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	10	
ARCHITECTURE-2h	ARCHITECTURE-2.h	N/A	All assets are segmented into distinct security zones based on cybersecurity requirements	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	8	
ARCHITECTURE-2i	ARCHITECTURE-2.i	N/A	Separate networks are implemented, where warranted, that logically or physically segment assets into security zones with independent authentication	Functional	Intersects With	Segregation From Enterprise Services	NET-06.4	Mechanisms exist to isolate sensitive/regulated data enclaves (secure zones) from corporate-provided IT resources by providing enclave-specific IT services (e.g., directory services, DNS, NTP, ITAM, antimalware, patch management, etc.) to those isolated network segments.	5	
ARCHITECTURE-2j	ARCHITECTURE-2.j	N/A	OT systems are operationally independent from IT systems so that OT operations can be sustained during an outage of IT systems	Functional	Subset Of	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	10	
ARCHITECTURE-2j	ARCHITECTURE-2.j	N/A	OT systems are operationally independent from IT systems so that OT operations can be sustained during an outage of IT systems	Functional	Intersects With	Segregation From Enterprise Services	NET-06.4	Mechanisms exist to isolate sensitive/regulated data enclaves (secure zones) from corporate-provided IT resources by providing enclave-specific IT services (e.g., directory services, DNS, NTP, ITAM, antimalware, patch management, etc.) to those isolated network segments.	8	
ARCHITECTURE-2k	ARCHITECTURE-2.k	N/A	Device connections to the network are controlled to ensure that only authorized devices can connect (for example, network access control (NAC))	Functional	Equal	Network Access Control (NAC)	AST-02.5	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	10	
ARCHITECTURE-2l	ARCHITECTURE-2.l	N/A	The cybersecurity architecture enables the isolation of compromised assets	Functional	Subset Of	Dynamic Isolation & Segregation (Sandboxing)	NET-03.6	Automated mechanisms exist to dynamically isolate (e.g., sandbox) untrusted components during runtime, where the component is isolated in a fault-contained environment but it can still collaborate with the application.	10	
ARCHITECTURE-3a	ARCHITECTURE-3.a	N/A	Logical and physical access controls are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	8	
ARCHITECTURE-3a	ARCHITECTURE-3.a	N/A	Logical and physical access controls are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	
ARCHITECTURE-3b	ARCHITECTURE-3.b	N/A	Endpoint protections (such as secure configuration, security applications, and host monitoring) are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner	Functional	Subset Of	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	10	
ARCHITECTURE-3b	ARCHITECTURE-3.b	N/A	Endpoint protections (such as secure configuration, security applications, and host monitoring) are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
ARCHITECTURE-3c	ARCHITECTURE-3.c	N/A	The principle of least privilege (for example, limiting administrative access for users and service accounts) is enforced	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.	8	
ARCHITECTURE-3c	ARCHITECTURE-3.c	N/A	The principle of least privilege (for example, limiting administrative access for users and service accounts) is enforced	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	8	
ARCHITECTURE-3d	ARCHITECTURE-3.d	N/A	The principle of least functionality (for example, limiting services, limiting applications, limiting ports, limiting connected devices) is enforced	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
ARCHITECTURE-3d	ARCHITECTURE-3.d	N/A	The principle of least functionality (for example, limiting services, limiting applications, limiting ports, limiting connected devices) is enforced	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	8	
ARCHITECTURE-3e	ARCHITECTURE-3.e	N/A	Secure configurations are established and maintained as part of the asset deployment process where feasible	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
ARCHITECTURE-3f	ARCHITECTURE-3.f	N/A	Security applications are required as an element of device configuration where feasible (for example, endpoint detection and response, host-based firewalls)	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
ARCHITECTURE-3f	ARCHITECTURE-3.f	N/A	Security applications are required as an element of device configuration where feasible (for example, endpoint detection and response, host-based firewalls)	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	8	
ARCHITECTURE-3g	ARCHITECTURE-3.g	N/A	The use of removeable media is controlled (for example, limiting the use of USB devices, managing external hard drives)	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
ARCHITECTURE-3g	ARCHITECTURE-3.g	N/A	The use of removeable media is controlled (for example, limiting the use of USB devices, managing external hard drives)	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	8	
ARCHITECTURE-3h	ARCHITECTURE-3.h	N/A	Cybersecurity controls are implemented for all assets within the function either at the asset level or as compensating controls where asset-level controls are not feasible	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	

FDE #	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
ARCHITECTURE-3h	ARCHITECTURE-3.h	N/A	Cybersecurity controls are implemented for all assets within the function either at the asset level or as compensating controls where asset-level controls are not feasible	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.	8	
ARCHITECTURE-3h	ARCHITECTURE-3.h	N/A	Cybersecurity controls are implemented for all assets within the function either at the asset level or as compensating controls where asset-level controls are not feasible	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	8	
ARCHITECTURE-3i	ARCHITECTURE-3.i	N/A	Maintenance and capacity management activities are performed for all assets within the function	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.	8	
ARCHITECTURE-3i	ARCHITECTURE-3.i	N/A	Maintenance and capacity management activities are performed for all assets within the function	Functional	Intersects With	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	8	
ARCHITECTURE-3j	ARCHITECTURE-3.j	N/A	The physical operating environment is controlled to protect the operation of assets within the function	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
ARCHITECTURE-3k	ARCHITECTURE-3.k	N/A	More rigorous cybersecurity controls are implemented for higher priority assets	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	
ARCHITECTURE-3l	ARCHITECTURE-3.l	N/A	Configuration of and changes to firmware are controlled throughout the asset lifecycle	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
ARCHITECTURE-3l	ARCHITECTURE-3.l	N/A	Configuration of and changes to firmware are controlled throughout the asset lifecycle	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	
ARCHITECTURE-3m	ARCHITECTURE-3.m	N/A	Controls (such as allowlists, blocklists, and configuration settings) are implemented to prevent the execution of unauthorized code	Functional	Subset Of	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10	
ARCHITECTURE-4a	ARCHITECTURE-4.a	N/A	Software developed in-house for deployment on higher priority assets is developed using secure software development practices	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	8	
ARCHITECTURE-4a	ARCHITECTURE-4.a	N/A	Software developed in-house for deployment on higher priority assets is developed using secure software development practices	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	8	
ARCHITECTURE-4b	ARCHITECTURE-4.b	N/A	The selection of procured software for deployment on higher priority assets includes consideration of the vendor's secure software development practices	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
ARCHITECTURE-4b	ARCHITECTURE-4.b	N/A	The selection of procured software for deployment on higher priority assets includes consideration of the vendor's secure software development practices	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
ARCHITECTURE-4b	ARCHITECTURE-4.b	N/A	The selection of procured software for deployment on higher priority assets includes consideration of the vendor's secure software development practices	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	
ARCHITECTURE-4c	ARCHITECTURE-4.c	N/A	Secure software configurations are required as part of the software deployment process for both procured software and software developed in-house	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:(1) Improve functionality;(2) Enhance security and resiliency capabilities;(3) Correct security deficiencies; and(4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
ARCHITECTURE-4c	ARCHITECTURE-4.c	N/A	Secure software configurations are required as part of the software deployment process for both procured software and software developed in-house	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	8	
ARCHITECTURE-4c	ARCHITECTURE-4.c	N/A	Secure software configurations are required as part of the software deployment process for both procured software and software developed in-house	Functional	Intersects With	Secure Settings By Default	TDA-09.6	Mechanisms exist to implement secure configuration settings by default to reduce the likelihood of Technology Assets, Applications and/or Services (TAAS) being deployed with weak security settings that would put the TAAS at a greater risk of compromise.	8	
ARCHITECTURE-4d	ARCHITECTURE-4.d	N/A	All software developed in-house is developed using secure software development practices	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
ARCHITECTURE-4e	ARCHITECTURE-4.e	N/A	The selection of all procured software includes consideration of the vendor's secure software development practices	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	8	
ARCHITECTURE-4e	ARCHITECTURE-4.e	N/A	The selection of all procured software includes consideration of the vendor's secure software development practices	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	8	
ARCHITECTURE-4e	ARCHITECTURE-4.e	N/A	The selection of all procured software includes consideration of the vendor's secure software development practices	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).	8	
ARCHITECTURE-4f	ARCHITECTURE-4.f	N/A	The architecture review process evaluates the security of new and revised applications prior to deployment	Functional	Intersects With	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that:(1) Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;(2) Accurately and completely describes the required security functionality and the allocation of security, compliance and resilience controls among physical and logical components; and(3) Expresses how individual security functions, mechanisms and services work together to provide required security capabilities and a unified approach to protection.	5	
ARCHITECTURE-4f	ARCHITECTURE-4.f	N/A	The architecture review process evaluates the security of new and revised applications prior to deployment	Functional	Intersects With	Software Design Review	TDA-06.5	Mechanisms exist to have an independent review of the software design to validate:(1) Applicable security, compliance and resilience requirements are met; and(2) Identified risks are remediated.	5	
ARCHITECTURE-4g	ARCHITECTURE-4.g	N/A	The authenticity of all software and firmware is validated prior to deployment	Functional	Subset Of	Software / Firmware Integrity Verification	TDA-14.1	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	10	
ARCHITECTURE-4h	ARCHITECTURE-4.h	N/A	Security testing (for example, static testing, dynamic testing, fuzz testing, penetration testing) is performed for in-house-developed and in-house-tailored applications periodically and according to defined triggers, such as system changes and external events	Functional	Subset Of	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results.	10	
ARCHITECTURE-4h	ARCHITECTURE-4.h	N/A	Security testing (for example, static testing, dynamic testing, fuzz testing, penetration testing) is performed for in-house-developed and in-house-tailored applications periodically and according to defined triggers, such as system changes and external events	Functional	Intersects With	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	8	
ARCHITECTURE-4h	ARCHITECTURE-4.h	N/A	Security testing (for example, static testing, dynamic testing, fuzz testing, penetration testing) is performed for in-house-developed and in-house-tailored applications periodically and according to defined triggers, such as system changes and external events	Functional	Intersects With	Dynamic Code Analysis	TDA-09.3	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.	8	
ARCHITECTURE-4h	ARCHITECTURE-4.h	N/A	Security testing (for example, static testing, dynamic testing, fuzz testing, penetration testing) is performed for in-house-developed and in-house-tailored applications periodically and according to defined triggers, such as system changes and external events	Functional	Intersects With	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications and/or Services (TAAS).	8	
ARCHITECTURE-5a	ARCHITECTURE-5.a	N/A	Sensitive data is protected at rest, at least in an ad hoc manner	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	8	
ARCHITECTURE-5b	ARCHITECTURE-5.b	N/A	All data at rest is protected for selected data categories	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	8	
ARCHITECTURE-5c	ARCHITECTURE-5.c	N/A	All data in transit is protected for selected data categories	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
ARCHITECTURE-5d	ARCHITECTURE-5.d	N/A	Cryptographic controls are implemented for data at rest and data in transit for selected data categories	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
ARCHITECTURE-5d	ARCHITECTURE-5.d	N/A	Cryptographic controls are implemented for data at rest and data in transit for selected data categories	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	8	
ARCHITECTURE-5d	ARCHITECTURE-5.d	N/A	Cryptographic controls are implemented for data at rest and data in transit for selected data categories	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
ARCHITECTURE-5e	ARCHITECTURE-5.e	N/A	Key management infrastructure (that is, key generation, key storage, key destruction, key update, and key revocation) is implemented to support cryptographic controls	Functional	Subset Of	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	10	
ARCHITECTURE-5f	ARCHITECTURE-5.f	N/A	Controls to restrict the exfiltration of data (for example, data loss prevention tools) are implemented	Functional	Intersects With	Prevent Unauthorized Exfiltration	NET-03.5	Automated mechanisms exist to prevent the unauthorized exfiltration of sensitive/regulated data across managed interfaces.	5	
ARCHITECTURE-5f	ARCHITECTURE-5.f	N/A	Controls to restrict the exfiltration of data (for example, data loss prevention tools) are implemented	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
ARCHITECTURE-5f	ARCHITECTURE-5.f	N/A	Controls to restrict the exfiltration of data (for example, data loss prevention tools) are implemented	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
ARCHITECTURE-5g	ARCHITECTURE-5.g	N/A	The cybersecurity architecture includes protections (such as full disk encryption) for data that is stored on assets that may be lost or stolen	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	
ARCHITECTURE-5h	ARCHITECTURE-5.h	N/A	The cybersecurity architecture includes protections against unauthorized changes to software, firmware, and data	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	
ARCHITECTURE-6a	ARCHITECTURE-6.a	N/A	Documented procedures are established, followed, and maintained for activities in the ARCHITECTURE domain	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	
ARCHITECTURE-6b	ARCHITECTURE-6.b	N/A	Adequate resources (people, funding, and tools) are provided to support activities in the ARCHITECTURE domain	Functional	Subset Of	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	
ARCHITECTURE-6c	ARCHITECTURE-6.c	N/A	Up-to-date policies or other organizational directives define requirements for activities in the ARCHITECTURE domain	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
ARCHITECTURE-6d	ARCHITECTURE-6.d	N/A	Responsibility, accountability, and authority for the performance of activities in the ARCHITECTURE domain are assigned to personnel	Functional	Subset Of	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	10	
ARCHITECTURE-6e	ARCHITECTURE-6.e	N/A	Personnel performing activities in the ARCHITECTURE domain have the skills and knowledge needed to perform their assigned responsibilities	Functional	Subset Of	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	10	
ARCHITECTURE-6f	ARCHITECTURE-6.f	N/A	The effectiveness of activities in the ARCHITECTURE domain is evaluated and tracked	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	10	
PROGRAM-1a	PROGRAM-1.a	N/A	The organization has a cybersecurity program strategy, which may be developed and managed in an ad hoc manner	Functional	Subset Of	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.	10	

FDE #	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
PROGRAM-1b	PROGRAM-1.b	N/A	The cybersecurity program strategy defines goals and objectives for the organization's cybersecurity activities	Functional	Subset Of	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.	10	
PROGRAM-1c	PROGRAM-1.c	N/A	The cybersecurity program strategy and priorities are documented and aligned with the organization's mission, strategic objectives, and risk to critical infrastructure	Functional	Subset Of	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.	10	
PROGRAM-1d	PROGRAM-1.d	N/A	The cybersecurity program strategy defines the organization's approach to provide program oversight and governance for cybersecurity activities	Functional	Subset Of	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.	10	
PROGRAM-1e	PROGRAM-1.e	N/A	The cybersecurity program strategy defines the structure and organization of the cybersecurity program	Functional	Subset Of	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.	10	
PROGRAM-1f	PROGRAM-1.f	N/A	The cybersecurity program strategy identifies standards and guidelines intended to be followed by the program	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
PROGRAM-1g	PROGRAM-1.g	N/A	The cybersecurity program strategy identifies any applicable compliance requirements that must be satisfied by the program (for example, NERC CIP, TSA Pipeline Security Guidelines, PCI DSS, ISO, DoD CMMC)	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
PROGRAM-1g	PROGRAM-1.g	N/A	The cybersecurity program strategy identifies any applicable compliance requirements that must be satisfied by the program (for example, NERC CIP, TSA Pipeline Security Guidelines, PCI DSS, ISO, DoD CMMC)	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
PROGRAM-1h	PROGRAM-1.h	N/A	The cybersecurity program strategy is updated periodically and according to defined triggers, such as business changes, changes in the operating environment, and changes in the threat profile (THREAT-2e)	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
PROGRAM-2a	PROGRAM-2.a	N/A	Senior management with proper authority provides support for the cybersecurity program, at least in an ad hoc manner	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	
PROGRAM-2b	PROGRAM-2.b	N/A	The cybersecurity program is established according to the cybersecurity program strategy	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	5	
PROGRAM-2c	PROGRAM-2.c	N/A	Senior management sponsorship for the cybersecurity program is visible and active	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	
PROGRAM-2d	PROGRAM-2.d	N/A	Senior management sponsorship is provided for the development, maintenance, and enforcement of cybersecurity policies	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	
PROGRAM-2e	PROGRAM-2.e	N/A	Responsibility for the cybersecurity program is assigned to a role with sufficient authority	Functional	Subset Of	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	10	
PROGRAM-2f	PROGRAM-2.f	N/A	Stakeholders for cybersecurity program management activities are identified and involved	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	
PROGRAM-2f	PROGRAM-2.f	N/A	Stakeholders for cybersecurity program management activities are identified and involved	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
PROGRAM-2g	PROGRAM-2.g	N/A	Cybersecurity program activities are periodically reviewed to ensure that they align with the cybersecurity program strategy	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5	
PROGRAM-2g	PROGRAM-2.g	N/A	Cybersecurity program activities are periodically reviewed to ensure that they align with the cybersecurity program strategy	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
PROGRAM-2h	PROGRAM-2.h	N/A	Cybersecurity activities are independently reviewed to ensure conformance with cybersecurity policies and procedures, periodically and according to defined triggers, such as process changes	Functional	Subset Of	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.	10	
PROGRAM-2i	PROGRAM-2.i	N/A	The cybersecurity program addresses and enables the achievement of legal and regulatory compliance, as appropriate	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
PROGRAM-2j	PROGRAM-2.j	N/A	The organization collaborates with external entities to contribute to the development and implementation of cybersecurity standards, guidelines, leading practices, lessons learned, and emerging technologies	Functional	Intersects With	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the security, compliance and resilience communities to:(1) Facilitate ongoing cybersecurity and data protection education and training for organizational personnel;(2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and(3) Share current cybersecurity and/or data protection-related information including threats, vulnerabilities and incidents.	3	
PROGRAM-3a	PROGRAM-3.a	N/A	Documented procedures are established, followed, and maintained for activities in the PROGRAM domain	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	
PROGRAM-3b	PROGRAM-3.b	N/A	Adequate resources (people, funding, and tools) are provided to support activities in the PROGRAM domain	Functional	Subset Of	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	
PROGRAM-3c	PROGRAM-3.c	N/A	Up-to-date policies or other organizational directives define requirements for activities in the PROGRAM domain	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
PROGRAM-3d	PROGRAM-3.d	N/A	Responsibility, accountability, and authority for the performance of activities in the PROGRAM domain are assigned to personnel	Functional	Subset Of	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	10	
PROGRAM-3e	PROGRAM-3.e	N/A	Personnel performing activities in the PROGRAM domain have the skills and knowledge needed to perform their assigned responsibilities	Functional	Subset Of	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	10	
PROGRAM-3f	PROGRAM-3.f	N/A	The effectiveness of activities in the PROGRAM domain is evaluated and tracked	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	10	