

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Security Controls Framework (SCF) Control Description	Strength of Relationship	Notes
A&A-01	Audit and Assurance Policies and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	
A&A-01	Audit and Assurance Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
A&A-02	Independent Assessments	Conduct independent audit and assurance assessments according to relevant standards at least annually.	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	
A&A-02	Independent Assessments	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Functional	Intersects With	Periodic Audits	CPL-02.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	8	
A&A-02	Independent Assessments	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	8	
A&A-02	Independent Assessments	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	8	
A&A-03	Risk Based Planning Assessment	Perform independent audit and assurance assessments according to risk-based plans and policies, and in response to significant changes or emerging risks.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	8	
A&A-04	Requirements Compliance	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
A&A-05	Audit Management Process	Define and implement an Audit Management process aligned with relevant auditing standards to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	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	
A&A-05	Audit Management Process	Define and implement an Audit Management process aligned with relevant auditing standards to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	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	
A&A-05	Audit Management Process	Define and implement an Audit Management process aligned with relevant auditing standards to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	8	
A&A-05	Audit Management Process	Define and implement an Audit Management process aligned with relevant auditing standards to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	8	
A&A-05	Audit Management Process	Define and implement an Audit Management process aligned with relevant auditing standards to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	5	
A&A-05	Audit Management Process	Define and implement an Audit Management process aligned with relevant auditing standards to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Functional	Intersects With	Functional Review Of Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	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	
A&A-05	Audit Management Process	Define and implement an Audit Management process aligned with relevant auditing standards to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Functional	Intersects With	Audit Activities	CPL-04	Mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations.	5	
A&A-06	Remediation	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, regularly review and report remediation status to relevant stakeholders.	Functional	Subset Of	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.	10	
A&A-06	Remediation	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, regularly review and report remediation status to relevant stakeholders.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	(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	
A&A-06	Remediation	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, regularly review and report remediation status to relevant stakeholders.	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	
A&A-06	Remediation	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, regularly review and report remediation status to relevant stakeholders.	Functional	Intersects With	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	5	
A&A-06	Remediation	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, regularly review and report remediation status to relevant stakeholders.	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
A&A-06	Remediation	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, regularly review and report remediation status to relevant stakeholders.	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.	5	
A&A-06	Remediation	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, regularly review and report remediation status to relevant stakeholders.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	
AIS-01	Application and Interface Security Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security. Review and update the policies and procedures at least annually, or upon significant changes.	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	
AIS-01	Application and Interface Security Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
AIS-01	Application and Interface Security Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security. Review and update the policies and procedures at least annually, or upon significant changes.	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	
AIS-02	Application Security Baseline Requirements	Establish, document and maintain baseline requirements for securing applications.	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	
AIS-02	Application Security Baseline Requirements	Establish, document and maintain baseline requirements for securing applications.	Functional	Intersects With	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes.	8	
AIS-02	Application Security Baseline Requirements	Establish, document and maintain baseline requirements for securing applications.	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	
AIS-02	Application Security Baseline Requirements	Establish, document and maintain baseline requirements for securing applications.	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	8	
AIS-02	Application Security Baseline Requirements	Establish, document and maintain baseline requirements for securing applications.	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	
AIS-02	Application Security Baseline Requirements	Establish, document and maintain baseline requirements for securing applications.	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.	5	
AIS-02	Application Security Baseline Requirements	Establish, document and maintain baseline requirements for securing applications.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
AIS-03	Application Security Metrics	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCR) measures of performance.	10	
AIS-04	Secure Application Development Lifecycle	Define and implement a secure SDLC process for application requirements analysis, planning, design, development, testing, deployment, and operation in accordance with security requirements.	Functional	Subset Of	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	10	
AIS-04	Secure Application Development Lifecycle	Define and implement a secure SDLC process for application requirements analysis, planning, design, development, testing, deployment, and operation in accordance with security requirements.	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	
AIS-04	Secure Application Development Lifecycle	Define and implement a secure SDLC process for application requirements analysis, planning, design, development, testing, deployment, and operation in accordance with security requirements.	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	8	
AIS-04	Secure Application Development Lifecycle	Define and implement a secure SDLC process for application requirements analysis, planning, design, development, testing, deployment, and operation in accordance with security requirements.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	8	
AIS-04	Secure Application Development Lifecycle	Define and implement a secure SDLC process for application requirements analysis, planning, design, development, testing, deployment, and operation in accordance with security requirements.	Functional	Intersects With	Secure Migration Practices	TDA-08.1	Mechanisms exist to ensure secure migration practices purge Technology Assets, Applications and/or Services (TAAS) of test/development/staging data and accounts before it is migrated into a production environment.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
AIS-04	Secure Application Development Lifecycle	Define and implement a secure SDLC process for application requirements analysis, planning, design, development, testing, deployment, and operation in accordance with security requirements.	Functional	Intersects With	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.	8	
AIS-05	Application Security Testing	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while meeting organizational delivery goals. Automate when applicable and possible.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Autonomous Technologies (AAT).	8	
AIS-05	Application Security Testing	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while meeting organizational delivery goals. Automate when applicable and possible.	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	
AIS-05	Application Security Testing	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while meeting organizational delivery goals. Automate when applicable and possible.	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	
AIS-05	Application Security Testing	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while meeting organizational delivery goals. Automate when applicable and possible.	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).	3	
AIS-06	Secure Application Deployment	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
AIS-06	Secure Application Deployment	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Functional	Intersects With	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modeling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5	
AIS-06	Secure Application Deployment	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Functional	Intersects With	Software Assurance Maturity Model (SAMM)	TDA-06.3	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS).	5	
AIS-06	Secure Application Deployment	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Functional	Intersects With	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	3	
AIS-06	Secure Application Deployment	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	3	
AIS-07	Application Vulnerability Remediation	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	Functional	Subset Of	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	10	
AIS-08	API Security	Define and implement processes, procedures, and technical measures to secure APIs. Review and update for any improvements at least annually or upon significant changes.	Functional	Subset Of	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	10	
BCR-01	Business Continuity Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually, or upon significant changes.	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	
BCR-01	Business Continuity Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
BCR-01	Business Continuity Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
BCR-02	Risk Assessment and Impact Analysis	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities. Review and update the risk assessment and impact analysis at least annually or upon significant changes.	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	
BCR-02	Risk Assessment and Impact Analysis	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities. Review and update the risk assessment and impact analysis at least annually or upon significant changes.	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	
BCR-02	Risk Assessment and Impact Analysis	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities. Review and update the risk assessment and impact analysis at least annually or upon significant changes.	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.	8	
BCR-02	Risk Assessment and Impact Analysis	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities. Review and update the risk assessment and impact analysis at least annually or upon significant changes.	Functional	Intersects With	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	8	
BCR-02	Risk Assessment and Impact Analysis	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities. Review and update the risk assessment and impact analysis at least annually or upon significant changes.	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	8	
BCR-03	Business Continuity Strategy	Establish strategies to reduce the impact of business disruptions, and improve resiliency and recovery from business disruptions.	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	
BCR-03	Business Continuity Strategy	Establish strategies to reduce the impact of business disruptions, and improve resiliency and recovery from business disruptions.	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	
BCR-03	Business Continuity Strategy	Establish strategies to reduce the impact of business disruptions, and improve resiliency and recovery from business disruptions.	Functional	Intersects With	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).	5	
BCR-03	Business Continuity Strategy	Establish strategies to reduce the impact of business disruptions, and improve resiliency and recovery from business disruptions.	Functional	Intersects With	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	8	
BCR-03	Business Continuity Strategy	Establish strategies to reduce the impact of business disruptions, and improve resiliency and recovery from business disruptions.	Functional	Intersects With	Continue Essential Mission & Business Functions	BCD-02.2	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites.	8	
BCR-03	Business Continuity Strategy	Establish strategies to reduce the impact of business disruptions, and improve resiliency and recovery from business disruptions.	Functional	Intersects With	Resume Essential Missions & Business Functions	BCD-02.3	Mechanisms exist to resume essential missions and business functions within an organization-defined time period of contingency plan activation.	8	
BCR-03	Business Continuity Strategy	Establish strategies to reduce the impact of business disruptions, and improve resiliency and recovery from business disruptions.	Functional	Intersects With	Provider Contingency Plan	BCD-10.3	Mechanisms exist to contractually-require external service providers to have contingency plans that meet organizational contingency requirements.	3	
BCR-03	Business Continuity Strategy	Establish strategies to reduce the impact of business disruptions, and improve resiliency and recovery from business disruptions.	Functional	Intersects With	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover capability, which is not collocated with the primary Technology Asset, Application and/or Service (TAAS), which can be activated with little-to-no loss of information or disruption to operations.	3	
BCR-03	Business Continuity Strategy	Establish strategies to reduce the impact of business disruptions, and improve resiliency and recovery from business disruptions.	Functional	Intersects With	Failover Capability	BCD-12.2	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical Technology Assets, Applications, Services and/or Data (TAASD).	3	
BCR-03	Business Continuity Strategy	Establish strategies to reduce the impact of business disruptions, and improve resiliency and recovery from business disruptions.	Functional	Intersects With	Restore Within Time Period	BCD-12.4	Mechanisms exist to restore Technology Assets, Applications, Services and/or Data (TAASD) within organization-defined restoration time-periods from configuration-controlled and integrity-protected information; representing a known, operational state for the asset.	8	
BCR-04	Business Continuity Planning	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	Functional	Intersects With	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.	8	
BCR-04	Business Continuity Planning	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	Functional	Intersects With	Contingency Planning Components	BCD-06.1	Mechanisms exist to identify components that potentially impact the organization's ability to execute contingency plans, including changes to: (1) Personnel roles; (2) Business processes (including the use of third-party services); (3) Deployed technologies; (4) Data repositories and/or data flows; and/or (5) Physical infrastructure.	8	

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
BCR-05	Documentation	Develop, identify, and acquire documentation, both internally and from external parties, that is relevant to support the business continuity and operational resilience plans. Make the documentation available to authorized stakeholders and review at least annually or upon significant changes.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	8	
BCR-05	Documentation	Develop, identify, and acquire documentation, both internally and from external parties, that is relevant to support the business continuity and operational resilience plans. Make the documentation available to authorized stakeholders and review at least annually or upon significant changes.	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and/or physical access to sensitive/regulated data.	5	
BCR-05	Documentation	Develop, identify, and acquire documentation, both internally and from external parties, that is relevant to support the business continuity and operational resilience plans. Make the documentation available to authorized stakeholders and review at least annually or upon significant changes.	Functional	Intersects With	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	5	
BCR-06	Business Continuity Exercises	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	Functional	Intersects With	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	5	
BCR-06	Business Continuity Exercises	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	Functional	Intersects With	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	5	
BCR-06	Business Continuity Exercises	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	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	
BCR-06	Business Continuity Exercises	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	Functional	Intersects With	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	5	
BCR-07	Communication	Establish and maintain communication channels with all relevant stakeholders in the course of business continuity and resilience procedures.	Functional	Intersects With	Recovery Operations Communications	BCD-01.6	Mechanisms exist to communicate the status of recovery activities and progress in restoring operational capabilities to designated internal and external stakeholders.	5	
BCR-08	Backup	Periodically perform backups. Ensure the confidentiality, integrity and availability of the backup, and verify restoration from backup for resiliency.	Functional	Subset Of	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).	10	
BCR-08	Backup	Periodically perform backups. Ensure the confidentiality, integrity and availability of the backup, and verify restoration from backup for resiliency.	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	
BCR-08	Backup	Periodically perform backups. Ensure the confidentiality, integrity and availability of the backup, and verify restoration from backup for resiliency.	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
BCR-08	Backup	Periodically perform backups. Ensure the confidentiality, integrity and availability of the backup, and verify restoration from backup for resiliency.	Functional	Intersects With	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	5	
BCR-09	Disaster Response Plan	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	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	
BCR-09	Disaster Response Plan	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	Functional	Intersects With	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.	8	
BCR-09	Disaster Response Plan	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	Functional	Intersects With	Contingency Planning Components	BCD-06.1	Mechanisms exist to identify components that potentially impact the organization's ability to execute contingency plans, including changes to: (1) Personnel roles; (2) Business processes (including the use of third-party services); (3) Deployed technologies; (4) Data repositories and/or data flows; and/or (5) Physical infrastructure.	3	
BCR-09	Disaster Response Plan	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	Functional	Intersects With	Contingency Plan Update Notifications	BCD-06.2	Mechanisms exist to keep stakeholders informed of changes to contingency plans.	3	
BCR-10	Response Plan Exercise	Exercise the disaster response plan annually or upon significant changes, including if possible, the participation of local emergency authorities.	Functional	Intersects With	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.	8	
BCR-11	Equipment Redundancy	Supplement business-critical equipment with both locally redundant and geographically dispersed equipment located at a reasonable minimum distance in accordance with applicable industry standards.	Functional	Intersects With	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover capability, which is not collocated with the primary Technology Asset, Application and/or Service (TAAS), which can be activated with little-to-no loss of information or disruption to operations.	8	
BCR-11	Equipment Redundancy	Supplement business-critical equipment with both locally redundant and geographically dispersed equipment located at a reasonable minimum distance in accordance with applicable industry standards.	Functional	Intersects With	Failover Capability	BCD-12.2	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical Technology Assets, Applications, Services and/or Data (TAASD).	8	
CCC-01	Change Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to assets owned, controlled or used by the organization. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and processes necessary for secure, compliant and resilient capabilities.	8	
CCC-01	Change Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to assets owned, controlled or used by the organization. Review and update the policies and procedures at least annually, or upon significant changes.	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.	8	
CCC-01	Change Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to assets owned, controlled or used by the organization. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	8	
CCC-02	Quality Testing	Establish, maintain and implement a defined quality change control, approval and testing process incorporating baselines, testing, and release standards.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	
CCC-02	Quality Testing	Establish, maintain and implement a defined quality change control, approval and testing process incorporating baselines, testing, and release standards.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a production environment before changes are implemented in a production environment.	8	
CCC-03	Change Management Technology	Implement a change management procedure to manage the risks associated with applying changes to assets, owned, controlled or used by the organization.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
CCC-03	Change Management Technology	Implement a change management procedure to manage the risks associated with applying changes to assets, owned, controlled or used by the organization.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	
CCC-03	Change Management Technology	Implement a change management procedure to manage the risks associated with applying changes to assets, owned, controlled or used by the organization.	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	5	
CCC-03	Change Management Technology	Implement a change management procedure to manage the risks associated with applying changes to assets, owned, controlled or used by the organization.	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.	5	
CCC-04	Unauthorized Change Protection	Implement and enforce a procedure to authorize the addition, removal, update, and management of assets that are owned, controlled or used by the organization.	Functional	Subset Of	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	10	
CCC-04	Unauthorized Change Protection	Implement and enforce a procedure to authorize the addition, removal, update, and management of assets that are owned, controlled or used by the organization.	Functional	Intersects With	Automated Security Response	CHG-02.4	Automated mechanisms exist to implement remediation actions upon the detection of unauthorized baseline configurations changes).	5	
CCC-04	Unauthorized Change Protection	Implement and enforce a procedure to authorize the addition, removal, update, and management of assets that are owned, controlled or used by the organization.	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	
CCC-04	Unauthorized Change Protection	Implement and enforce a procedure to authorize the addition, removal, update, and management of assets that are owned, controlled or used by the organization.	Functional	Intersects With	Automated Access Enforcement / Auditing	CHG-04.1	Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes.	5	
CCC-04	Unauthorized Change Protection	Implement and enforce a procedure to authorize the addition, removal, update, and management of assets that are owned, controlled or used by the organization.	Functional	Intersects With	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.	8	
CCC-05	Change Agreements	Include provisions limiting changes directly impacting service customers owned environments (tenants) to explicitly authorized requests within service level agreements.	Functional	Subset Of	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	10	
CCC-05	Change Agreements	Include provisions limiting changes directly impacting service customers owned environments (tenants) to explicitly authorized requests within service level agreements.	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.	5	
CCC-05	Change Agreements	Include provisions limiting changes directly impacting service customers owned environments (tenants) to explicitly authorized requests within service level agreements.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5	
CCC-06	Change Management Baseline	Establish, document and implement change management and configuration baselines for all relevant authorized changes on organization assets. Review and update the baselines at least annually or upon significant changes.	Functional	Intersects With	Automated Security Response	CHG-02.4	Automated mechanisms exist to implement remediation actions upon the detection of unauthorized baseline configurations changes).	5	
CCC-06	Change Management Baseline	Establish, document and implement change management and configuration baselines for all relevant authorized changes on organization assets. Review and update the baselines at least annually or upon significant changes.	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	
CCC-06	Change Management Baseline	Establish, document and implement change management and configuration baselines for all relevant authorized changes on organization assets. Review and update the baselines at least annually or upon significant changes.	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	
CCC-06	Change Management Baseline	Establish, document and implement change management and configuration baselines for all relevant authorized changes on organization assets. Review and update the baselines at least annually or upon significant changes.	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.	8	
CCC-07	Detection of Baseline Deviation	Implement detection measures with proactive notification in case of changes deviating from the established baseline.	Functional	Subset Of	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.	10	
CCC-08	Exception Management	Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.	Functional	Subset Of	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	10	
CCC-08	Exception Management	Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.	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.	3	

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
CCC-08	Exception Management	Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	8	
CCC-09	Change Restoration	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	Functional	Subset Of	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	10	
CCC-09	Change Restoration	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	Functional	Intersects With	Automated Security Response	CHG-02.4	Automated mechanisms exist to implement remediation actions upon the detection of unauthorized baseline configurations changes.	5	
CCC-09	Change Restoration	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	Functional	Intersects With	Automated Access Enforcement / Auditing	CHG-04.1	Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes.	5	
CCC-09	Change Restoration	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	Functional	Intersects With	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.	5	
CEK-01	Encryption and Key Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	
CEK-01	Encryption and Key Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
CEK-01	Encryption and Key Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	8	
CEK-02	CEK Roles and Responsibilities	Define and implement cryptographic, encryption and key management roles and responsibilities.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	3	
CEK-02	CEK Roles and Responsibilities	Define and implement cryptographic, encryption and key management roles and responsibilities.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
CEK-02	CEK Roles and Responsibilities	Define and implement cryptographic, encryption and key management roles and responsibilities.	Functional	Intersects With	Incompatible Roles	HRS-12	Mechanisms exist to avoid incompatible development-specific roles through limiting and reviewing developer privileges to change hardware, software and firmware components within a production/operational environment.	5	
CEK-03	Data Protection	Provide data protection at-rest, in-transit, and where applicable, in-use by using cryptographic libraries certified to approved standards.	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	
CEK-03	Data Protection	Provide data protection at-rest, in-transit, and where applicable, in-use by using cryptographic libraries certified to approved standards.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
CEK-03	Data Protection	Provide data protection at-rest, in-transit, and where applicable, in-use by using cryptographic libraries certified to approved standards.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	8	
CEK-04	Encryption Algorithm	Utilize encryption algorithms following industry standards for protecting data, based on the data classification and associated risks.	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	
CEK-04	Encryption Algorithm	Utilize encryption algorithms following industry standards for protecting data, based on the data classification and associated risks.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
CEK-05	Encryption Change Management	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	Functional	Subset Of	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	10	
CEK-06	Encryption Change Cost Benefit Analysis	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
CEK-06	Encryption Change Cost Benefit Analysis	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5	
CEK-07	Encryption Risk Management	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
CEK-07	Encryption Risk Management	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	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	
CEK-07	Encryption Risk Management	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Functional	Intersects With	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	5	
CEK-07	Encryption Risk Management	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
CEK-07	Encryption Risk Management	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	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	
CEK-07	Encryption Risk Management	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
CEK-07	Encryption Risk Management	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Functional	Intersects With	Risk Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.	5	
CEK-07	Encryption Risk Management	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
CEK-07	Encryption Risk Management	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Functional	Intersects With	Risk Response	RSK-06.1	Immediate findings from security, compliance and/or resilience-related: 1) Assessments; 2) Audits; and/or	5	
CEK-08	Service Customer Key Management Capability	Service providers must provide the capability for service customers to manage their own data encryption keys.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	8	
CEK-08	Service Customer Key Management Capability	Service providers must provide the capability for service customers to manage their own data encryption keys.	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	
CEK-09	Encryption and Key Management Audit	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and upon any security events.	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	
CEK-09	Encryption and Key Management Audit	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and upon any security events.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	8	
CEK-09	Encryption and Key Management Audit	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and upon any security events.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	8	
CEK-09	Encryption and Key Management Audit	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and upon any security events.	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	5	
CEK-09	Encryption and Key Management Audit	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and upon any security 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.	8	
CEK-10	Key Generation	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	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	
CEK-10	Key Generation	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	Functional	Intersects With	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	8	
CEK-11	Key Purpose	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	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	
CEK-11	Key Purpose	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	Functional	Intersects With	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	5	
CEK-12	Key Rotation	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	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	
CEK-12	Key Rotation	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5	
CEK-12	Key Rotation	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	Functional	Intersects With	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	5	
CEK-13	Key Revocation	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	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	
CEK-13	Key Revocation	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	8	
CEK-14	Key Destruction	Define, implement, and evaluate processes, procedures, and technical measures to securely destroy cryptographic keys when they are no longer needed, which include provisions for legal and regulatory requirements.	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	
CEK-14	Key Destruction	Define, implement, and evaluate processes, procedures, and technical measures to securely destroy cryptographic keys when they are no longer needed, which include provisions for legal and regulatory requirements.	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	8	
CEK-15	Key Activation	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	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	

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
CEK-15	Key Activation	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	8	
CEK-15	Key Activation	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	Functional	Intersects With	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	8	
CEK-16	Key Suspension	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.	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	
CEK-16	Key Suspension	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	8	
CEK-17	Key Deactivation	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.	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	
CEK-17	Key Deactivation	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	8	
CEK-18	Key Archival	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.	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	
CEK-19	Key Compromise	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.	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	
CEK-19	Key Compromise	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	8	
CEK-20	Key Recovery	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.	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	
CEK-21	Key Inventory Management	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.	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	
DCS-01	Physical and Environmental Security Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for physical and environmental security. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	
DCS-01	Physical and Environmental Security Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for physical and environmental security. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
DCS-01	Physical and Environmental Security Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for physical and environmental security. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	
DCS-02	Off-Site Equipment Disposal Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually, or upon significant changes.	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	
DCS-02	Off-Site Equipment Disposal Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	8	
DCS-02	Off-Site Equipment Disposal Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually, or upon significant changes.	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	
DCS-03	Off-Site Transfer Authorization Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Security of Assets & Media	AST-05	Mechanisms exist to maintain strict control over the internal or external distribution of any kind of sensitive/regulated media.	5	
DCS-03	Off-Site Transfer Authorization Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Management Approval For External Media Transfer	AST-05.1	Mechanisms exist to obtain management approval for any sensitive/regulated media that is transferred outside of the organization's facilities.	5	
DCS-03	Off-Site Transfer Authorization Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Transfer to Alternate Storage Site	BCD-11.6	Mechanisms exist to transfer backup data to the alternate storage site at a rate that is capable of meeting both Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
DCS-03	Off-Site Transfer Authorization Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Transfer of Sensitive and/or Regulated Data	DCH-25	Mechanisms exist to restrict and govern the transfer of sensitive and/or regulated data to third-country or international organizations.	5	
DCS-04	Secure Area Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	8	
DCS-04	Secure Area Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	8	
DCS-05	Secure Media Transportation Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	8	
DCS-05	Secure Media Transportation Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	8	
DCS-05	Secure Media Transportation Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Encrypting Data in Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	5	
DCS-06	Assets Classification	Classify and document the physical and logical assets (e.g., applications) based on the organizational business risk. Review and update the assets' classification at least annually, or upon significant changes.	Functional	Subset Of	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	10	
DCS-07	Assets Cataloging and Tracking	Catalogue and track all relevant physical and logical assets located at all of the service provider's sites within a secured system. Review and update the catalogue at least annually or upon significant 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	
DCS-08	Controlled Physical Access Points	Design and implement physical security perimeters to safeguard personnel, data, and information systems.	Functional	Subset Of	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).	10	
DCS-08	Controlled Physical Access Points	Design and implement physical security perimeters to safeguard personnel, data, and information systems.	Functional	Intersects With	Controlled Ingress & Egress Points	PES-03.1	Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.	8	
DCS-09	Equipment Identification	Use equipment identification as a method for connection authentication.	Functional	Intersects With	Standardized Naming Convention	AST-01.3	Mechanisms exist to implement a scalable, standardized naming convention for Technology Assets, Applications, Services and/or Data (TAASD) that avoids asset naming conflicts.	8	
DCS-09	Equipment Identification	Use equipment identification as a method for connection authentication.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally authenticate, authorize and audit (AAI) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.	8	
DCS-10	Secure Area Authorization	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	8	
DCS-10	Secure Area Authorization	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	8	

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
DCS-10	Secure Area Authorization	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	Functional	Intersects With	Monitoring Physical Access	PE5-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	8	
DCS-11	Surveillance System	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.	Functional	Intersects With	Monitoring Physical Access	PE5-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	8	
DCS-11	Surveillance System	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.	Functional	Intersects With	Intrusion Alarms / Surveillance Equipment	PE5-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	8	
DCS-12	Adverse Event Response Training	Train datacenter personnel to safely manage adverse events, including but not limited to unauthorized ingress and egress attempts.	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	
DCS-13	Cabling Security	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.	Functional	Subset Of	Transmission Medium Security	PE5-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
DCS-14	Environmental Systems	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Functional	Subset Of	Supporting Utilities	PE5-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	10	
DCS-14	Environmental Systems	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Functional	Intersects With	Automatic Voltage Controls	PE5-07.1	Facility security mechanisms exist to utilize automatic voltage controls for critical system components.	5	
DCS-14	Environmental Systems	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Functional	Intersects With	Emergency Shutoff	PE5-07.2	Facility security mechanisms exist to shut off power in emergency situations by: (1) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and (2) Protecting emergency power shutoff capability from unauthorized activation.	5	
DCS-14	Environmental Systems	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Functional	Intersects With	Emergency Power	PE5-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	5	
DCS-14	Environmental Systems	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Functional	Intersects With	Emergency Lighting	PE5-07.4	Facility security mechanisms exist to utilize and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	5	
DCS-14	Environmental Systems	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Functional	Intersects With	Water Damage Protection	PE5-07.5	Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key personnel.	5	
DCS-15	Secure Utilities	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.	Functional	Intersects With	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.	8	
DCS-15	Secure Utilities	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.	Functional	Intersects With	Supporting Utilities	PE5-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	8	
DCS-16	Equipment Location	Keep business-critical equipment away from locations subject to high probability for environmental risk events.	Functional	Subset Of	Equipment Siting & Protection	PE5-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	10	
DCS-17	Datacenter Metrics	Establish, monitor and report datacenter security metrics to secure data center assets and services.	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRIP) measures of performance.	10	
DCS-18	Datacenter Operations Resilience	Define, implement and evaluate processes, procedures and technical measures to ensure continuous operations.	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	
DCS-18	Datacenter Operations Resilience	Define, implement and evaluate processes, procedures and technical measures to ensure continuous operations.	Functional	Intersects With	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	8	
DCS-18	Datacenter Operations Resilience	Define, implement and evaluate processes, procedures and technical measures to ensure continuous operations.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to ensure resistance to: (1) Unintentional errors (by users or software); and (2) Intentional attack or circumvention.	8	
DSP-01	Security and Privacy Policy and Stewardship	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the preparation, classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually, or upon significant changes.	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	
DSP-02	Secure Disposal	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	Functional	Subset Of	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.	10	
DSP-03	Data Inventory	Create and maintain a data inventory, at least for any sensitive, regulated and personal data. Review and update the inventory at least annually or upon significant 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	
DSP-04	Data Classification	Classify data according to its type, criticality and sensitivity level.	Functional	Subset Of	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	10	
DSP-05	Data Flow Documentation	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, or upon significant changes.	Functional	Subset Of	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/registed data flows.	10	
DSP-06	Data Ownership and Stewardship	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	Functional	Intersects With	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	8	
DSP-07	Data Protection by Design and Default	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	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	
DSP-07	Data Protection by Design and Default	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	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	
DSP-08	Data Privacy by Design and Default	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	8	
DSP-08	Data Privacy by Design and Default	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	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	
DSP-09	Data Protection Impact Assessment	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.	Functional	Equal	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
DSP-10	Sensitive Data Transfer	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
DSP-10	Sensitive Data Transfer	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
DSP-10	Sensitive Data Transfer	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
DSP-10	Sensitive Data Transfer	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Functional	Intersects With	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	8	
DSP-10	Sensitive Data Transfer	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Functional	Intersects With	Transfer Authorizations	DCH-14.2	Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between interconnected TAAS have the requisite authorizations (e.g., write permissions or privileges) prior to transferring said data.	8	
DSP-10	Sensitive Data Transfer	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Functional	Intersects With	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	8	
DSP-11	Personal Data Access, Reversal, Rectification and Deletion	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
DSP-12	Limitation of Purpose in Personal Data Processing	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Functional	Intersects With	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purposes for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	8	
DSP-12	Limitation of Purpose in Personal Data Processing	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Functional	Intersects With	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a specific business process.	8	
DSP-12	Limitation of Purpose in Personal Data Processing	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.	8	
DSP-12	Limitation of Purpose in Personal Data Processing	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	8	
DSP-13	Personal Data Sub-processing	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Functional	Intersects With	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	8	
DSP-13	Personal Data Sub-processing	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	8	
DSP-13	Personal Data Sub-processing	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Functional	Intersects With	Joint Processing of Personal Data (PD)	PRI-07.2	Mechanisms exist to clearly define and communicate the organization's role in processing Personal Data (PD) in the data processing ecosystem.	5	
DSP-13	Personal Data Sub-processing	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Functional	Intersects With	Obligation To Inform Third-Parties	PRI-07.3	Mechanisms exist to inform applicable third-parties of any modification, deletion or other change that affects shared Personal Data (PD).	5	
DSP-14	Disclosure of Data Sub-processors	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	8	
DSP-15	Limitation of Production Data Use	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.	8	
DSP-15	Limitation of Production Data Use	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	Functional	Intersects With	Use of Live Data	TDA-10	Mechanisms exist to approve, document and control the use of live data in development and test environments.	5	
DSP-16	Data Retention and Deletion	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	Functional	Subset Of	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	10	
DSP-16	Data Retention and Deletion	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	8	
DSP-17	Sensitive Data Protection	Define and implement, processes, procedures and technical measures to protect sensitive data throughout its lifecycle.	Functional	Intersects With	Sensitive Data in Public Cloud Providers	CLD-10	Mechanisms exist to limit and manage the storage of sensitive/regulatory data in public cloud providers.	5	
DSP-17	Sensitive Data Protection	Define and implement, processes, procedures and technical measures to protect sensitive data throughout its lifecycle.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
DSP-17	Sensitive Data Protection	Define and implement, processes, procedures and technical measures to protect sensitive data throughout its lifecycle.	Functional	Intersects With	Highest Classification Level	DCH-02.1	Mechanisms exist to ensure that Technology Assets, Applications and/or Services (TAAS) are classified according to the highest level of data sensitivity that is stored, transmitted and/or processed.	5	
DSP-17	Sensitive Data Protection	Define and implement, processes, procedures and technical measures to protect sensitive data throughout its lifecycle.	Functional	Intersects With	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and product sensitive media inventories at least annually.	5	
DSP-17	Sensitive Data Protection	Define and implement, processes, procedures and technical measures to protect sensitive data throughout its lifecycle.	Functional	Intersects With	Making Sensitive Data Unreadable in Storage	DCH-06.4	Mechanisms exist to ensure sensitive/regulatory data is rendered human unreadable anywhere sensitive/regulatory data is stored.	5	
DSP-17	Sensitive Data Protection	Define and implement, processes, procedures and technical measures to protect sensitive data throughout its lifecycle.	Functional	Intersects With	Protecting Sensitive / Regulated Data on External Technology Assets, Applications and/or Services (TAAS)	DCH-13.3	Mechanisms exist to ensure that the requirements for the protection of sensitive/regulatory data processed, stored or transmitted on external Technology Assets, Applications and/or Services (TAAS), are implemented in accordance with applicable statutory, regulatory and contractual obligations.	5	
DSP-17	Sensitive Data Protection	Define and implement, processes, procedures and technical measures to protect sensitive data throughout its lifecycle.	Functional	Intersects With	Access To Sensitive / Regulated Data	IAC-20.1	Mechanisms exist to limit access to sensitive/regulatory data to only those individuals whose job requires such access.	5	
DSP-17	Sensitive Data Protection	Define and implement, processes, procedures and technical measures to protect sensitive data throughout its lifecycle.	Functional	Intersects With	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive/regulatory data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
DSP-17	Sensitive Data Protection	Define and implement, processes, procedures and technical measures to protect sensitive data throughout its lifecycle.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
DSP-17	Sensitive Data Protection	Define and implement, processes, procedures and technical measures to protect sensitive data throughout its lifecycle.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulatory data is formally trained in data handling requirements.	5	
DSP-18	Disclosure Notification	The service provider must implement and describe to service customers the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations	Functional	Intersects With	Legal Assessment of Investigative Inquires	CPL-05	Mechanisms exist to determine whether a government agency has an applicable and valid legal basis to request data from the organization and what further steps need to be taken, if necessary.	8	
DSP-18	Disclosure Notification	The service provider must implement and describe to service customers the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations	Functional	Intersects With	Investigation Request Notifications	CPL-05.1	Mechanisms exist to notify customers about investigation request notifications, unless the applicable legal basis for a government agency's action prohibits notification (e.g., potential criminal prosecution).	8	
DSP-18	Disclosure Notification	The service provider must implement and describe to service customers the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations	Functional	Intersects With	Investigation Access Restrictions	CPL-05.2	Mechanisms exist to support official investigations by provisioning government investigators with "least privileges" and "least functionality" to ensure that government investigators only have access to the Technology Assets, Applications, Services and/or Data (TAASD) needed to perform the investigation.	8	
DSP-18	Disclosure Notification	The service provider must implement and describe to service customers the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations	Functional	Intersects With	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulatory data to authorized parties with a need to know.	8	
DSP-18	Disclosure Notification	The service provider must implement and describe to service customers the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations	Functional	Intersects With	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	5	
DSP-18	Disclosure Notification	The service provider must implement and describe to service customers the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations	Functional	Intersects With	Justification To Reject Disclosure Requests	PRI-07.5	Mechanisms exist to reject data subject access requests that are categorized as: (1) Harassing; (2) Repetitive; or (3) Fraudulent.	5	
DSP-18	Disclosure Notification	The service provider must implement and describe to service customers the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations	Functional	Intersects With	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by: (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.	8	
DSP-18	Disclosure Notification	The service provider must implement and describe to service customers the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations	Functional	Intersects With	Notification of Disclosure Request To Data Subject	PRI-14.2	Mechanisms exist to notify data subjects of applicable legal requests to disclose Personal Data (PD).	8	
DSP-19	Data Location	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
DSP-19	Data Location	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	Functional	Subset Of	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	10	
GRC-01	Governance Program Policies and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRPR)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
GRC-01	Governance Program Policies and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	

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
GRC-02	Risk Management Program	Establish and maintain a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of risks.	Functional	Intersects With	Risk Management Program	RISK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
GRC-03	Organizational Policy Reviews	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.	Functional	Equal	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	10	
GRC-04	Policy Exception Process	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.	Functional	Subset Of	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	10	
GRC-05	Information Security Program	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.	Functional	Subset Of	Security, Compliance & Resilience Program (SCR)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
GRC-06	Governance Responsibility Model	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	Functional	Intersects With	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 (SCR).	8	
GRC-06	Governance Responsibility Model	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	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.	8	
GRC-06	Governance Responsibility Model	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	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	
GRC-06	Governance Responsibility Model	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
GRC-06	Governance Responsibility Model	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASC) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	
GRC-07	Information System Regulatory Mapping	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization. Review at least annually or upon significant changes.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
GRC-07	Information System Regulatory Mapping	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization. Review at least annually or upon significant changes.	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	8	
GRC-08	Special Interest Groups	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.	Functional	Subset Of	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.	10	
HRS-01	Background Screening Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
HRS-01	Background Screening Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	8	
HRS-02	Acceptable Use of Technology Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Subset Of	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.	10	
HRS-02	Acceptable Use of Technology Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually, or upon significant changes.	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	
HRS-02	Acceptable Use of Technology Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually, or upon significant changes.	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	
HRS-03	Clean Desk Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually, or upon significant changes.	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.	5	
HRS-04	Remote and Home Working Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information and assets stored or stored at remote sites and locations. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Subset Of	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	10	
HRS-05	Asset returns	Establish and document procedures for the return of organization-owned assets by terminated employees, contractors and third parties.	Functional	Subset Of	Return of Assets	AST-10	Mechanisms exist to ensure that employees and third-party users return all organizational assets in their possession upon termination of employment, contract or agreement.	10	
HRS-06	Employment Termination	Establish, document, and communicate to all relevant personnel the procedures outlining the roles and responsibilities concerning changes in employment.	Functional	Subset Of	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	10	
HRS-06	Employment Termination	Establish, document, and communicate to all relevant personnel the procedures outlining the roles and responsibilities concerning changes in employment.	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	8	
HRS-07	Employment Agreement Process	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	Functional	Intersects With	Formal Indoctination	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.	5	
HRS-07	Employment Agreement Process	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	Functional	Subset Of	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.	10	
HRS-08	Employment Agreement Content	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.	Functional	Subset Of	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.	10	
HRS-08	Employment Agreement Content	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.	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	
HRS-09	Personnel Roles and Responsibilities	Establish, document and communicate roles and responsibilities of employees, as they relate to information assets' security and privacy.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
HRS-10	Non-Disclosure Agreements	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.	Functional	Subset Of	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	10	
HRS-11	Security Awareness Training	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
HRS-12	Personal and Sensitive Data Awareness and Training	Provide employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	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	
HRS-13	Compliance User Responsibility	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	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	
HRS-13	Compliance User Responsibility	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	Functional	Intersects With	Formal Indoctination	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	
HRS-13	Compliance User Responsibility	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	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	
IAM-01	Identity and Access Management Policy and Procedures	Establish, document, approve, communicate, implement, apply, evaluate, and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	
IAM-01	Identity and Access Management Policy and Procedures	Establish, document, approve, communicate, implement, apply, evaluate, and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
IAM-01	Identity and Access Management Policy and Procedures	Establish, document, approve, communicate, implement, apply, evaluate, and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	8	
IAM-01	Identity and Access Management Policy and Procedures	Establish, document, approve, communicate, implement, apply, evaluate, and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	5	
IAM-02	Credentials Management Policy and Procedures	Establish, document, approve, communicate, implement, apply, evaluate, and maintain policies and procedures for the management of authentication credentials, including passwords. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	

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
IAM-02	Credentials Management Policy and Procedures	Establish, document, approve, communicate, implement, apply, evaluate, and maintain policies and procedures for the management of authentication credentials, including passwords. Review and update the policies and procedures at least annually, or upon significant changes.	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.	8	
IAM-02	Credentials Management Policy and Procedures	Establish, document, approve, communicate, implement, apply, evaluate, and maintain policies and procedures for the management of authentication credentials, including passwords. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	8	
IAM-03	Identity Inventory	Manage, store, and regularly review the inventory of identities, and monitor their level of access.	Functional	Intersects With	User & Service Account Inventories	IAC-01.3	Mechanisms exist to maintain a current list of authorized users and service accounts.	8	
IAM-03	Identity Inventory	Manage, store, and regularly review the inventory of identities, and monitor their level of access.	Functional	Intersects With	Privileged Account Inventories	IAC-16.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	8	
IAM-04	Separation of Duties	Employ the separation of duties principle when implementing information system access.	Functional	Equal	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	10	
IAM-05	Least Privilege	Employ the least privilege principle when implementing information system access.	Functional	Equal	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.	10	
IAM-06	Access Provisioning	Define and implement an identity access provisioning process which authorizes, records, and communicates access changes to data and assets.	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	
IAM-07	Access Changes and Revocation	De-provision or modify identity access in a timely manner.	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.	5	
IAM-07	Access Changes and Revocation	De-provision or modify identity access in a timely manner.	Functional	Intersects With	High-Risk Terminations	HRS-09.2	Mechanisms exist to expedite the process of removing "high risk" individual's access to Technology Assets, Applications, Services and/or Data (TAASD) upon termination, as determined by management.	5	
IAM-07	Access Changes and Revocation	De-provision or modify identity access in a timely manner.	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	
IAM-07	Access Changes and Revocation	De-provision or modify identity access in a timely manner.	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	
IAM-07	Access Changes and Revocation	De-provision or modify identity access in a timely manner.	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	
IAM-07	Access Changes and Revocation	De-provision or modify identity access in a timely manner.	Functional	Intersects With	Account Disabling for High Risk Individuals	IAC-15.6	Mechanisms exist to disable accounts immediately upon notification for users posing a significant risk to the organization.	5	
IAM-08	Access Review	Review and reevaluate identity access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance, and at least annually or upon significant changes.	Functional	Subset Of	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.	10	
IAM-09	Segregation of Privileged Access Roles	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles.	Functional	Intersects With	Restrict Roles Permitted To Install Software	CFG-05.2	Mechanisms exist to configure systems to prevent the installation of software, unless the action is performed by a privileged user or service.	5	
IAM-09	Segregation of Privileged Access Roles	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles.	Functional	Intersects With	Privileged User Oversight	MON-01.15	Mechanisms exist to implement enhanced activity monitoring for privileged users.	5	
IAM-09	Segregation of Privileged Access Roles	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles.	Functional	Intersects With	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	5	
IAM-09	Segregation of Privileged Access Roles	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles.	Functional	Subset Of	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.	10	
IAM-09	Segregation of Privileged Access Roles	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles.	Functional	Intersects With	Privileged Account Identifiers	IAC-09.5	Mechanisms exist to uniquely manage privileged accounts to identify the account as a privileged user or service.	5	
IAM-09	Segregation of Privileged Access Roles	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles.	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	
IAM-09	Segregation of Privileged Access Roles	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles.	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	
IAM-09	Segregation of Privileged Access Roles	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles.	Functional	Intersects With	Authorize Access to Security Functions	IAC-21.1	Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.	5	
IAM-09	Segregation of Privileged Access Roles	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles.	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.	5	
IAM-09	Segregation of Privileged Access Roles	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles.	Functional	Intersects With	Auditing Use of Privileged Functions	IAC-21.4	Mechanisms exist to audit the execution of privileged functions.	5	
IAM-09	Segregation of Privileged Access Roles	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles.	Functional	Intersects With	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	5	
IAM-09	Segregation of Privileged Access Roles	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles.	Functional	Intersects With	Privileged Access	VPM-06.3	Mechanisms exist to implement privileged access authorization for selected vulnerability scanning activities.	3	
IAM-10	Management of Privileged Access Roles	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the accumulation of segregated privileged access.	Functional	Intersects With	Privileged User Oversight	MON-01.15	Mechanisms exist to implement enhanced activity monitoring for privileged users.	8	
IAM-10	Management of Privileged Access Roles	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the accumulation of segregated privileged access.	Functional	Intersects With	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	5	
IAM-10	Management of Privileged Access Roles	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the accumulation of segregated privileged access.	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	
IAM-10	Management of Privileged Access Roles	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the accumulation of segregated privileged access.	Functional	Intersects With	Privileged Account Identifiers	IAC-09.5	Mechanisms exist to uniquely manage privileged accounts to identify the account as a privileged user or service.	5	
IAM-10	Management of Privileged Access Roles	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the accumulation of segregated privileged access.	Functional	Subset Of	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).	10	
IAM-10	Management of Privileged Access Roles	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the accumulation of segregated privileged access.	Functional	Intersects With	Privileged Account Inventories	IAC-16.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	8	
IAM-10	Management of Privileged Access Roles	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the accumulation of segregated privileged access.	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	
IAM-11	Service Customers Approval for Agreed Privileged Access Roles	Define, implement and evaluate processes and procedures for service customers to participate, where applicable, in the granting of access for agreed, high risk as defined by the organizational risk assessment) privileged access roles.	Functional	Intersects With	Privileged User Oversight	MON-01.15	Mechanisms exist to implement enhanced activity monitoring for privileged users.	5	
IAM-11	Service Customers Approval for Agreed Privileged Access Roles	Define, implement and evaluate processes and procedures for service customers to participate, where applicable, in the granting of access for agreed, high risk as defined by the organizational risk assessment) privileged access roles.	Functional	Intersects With	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	5	
IAM-11	Service Customers Approval for Agreed Privileged Access Roles	Define, implement and evaluate processes and procedures for service customers to participate, where applicable, in the granting of access for agreed, high risk as defined by the organizational risk assessment) privileged access roles.	Functional	Intersects With	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5	
IAM-11	Service Customers Approval for Agreed Privileged Access Roles	Define, implement and evaluate processes and procedures for service customers to participate, where applicable, in the granting of access for agreed, high risk as defined by the organizational risk assessment) privileged access roles.	Functional	Intersects With	Privileged Account Identifiers	IAC-09.5	Mechanisms exist to uniquely manage privileged accounts to identify the account as a privileged user or service.	5	
IAM-11	Service Customers Approval for Agreed Privileged Access Roles	Define, implement and evaluate processes and procedures for service customers to participate, where applicable, in the granting of access for agreed, high risk as defined by the organizational risk assessment) privileged access roles.	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	
IAM-11	Service Customers Approval for Agreed Privileged Access Roles	Define, implement and evaluate processes and procedures for service customers to participate, where applicable, in the granting of access for agreed, high risk as defined by the organizational risk assessment) privileged access roles.	Functional	Intersects With	Privileged Account Inventories	IAC-16.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	5	
IAM-11	Service Customers Approval for Agreed Privileged Access Roles	Define, implement and evaluate processes and procedures for service customers to participate, where applicable, in the granting of access for agreed, high risk as defined by the organizational risk assessment) privileged access roles.	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	
IAM-11	Service Customers Approval for Agreed Privileged Access Roles	Define, implement and evaluate processes and procedures for service customers to participate, where applicable, in the granting of access for agreed, high risk as defined by the organizational risk assessment) privileged access roles.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
IAM-11	Service Customers Approval for Agreed Privileged Access Roles	Define, implement and evaluate processes and procedures for service customers to participate, where applicable, in the granting of access for agreed, high risk as defined by the organizational risk assessment) privileged access roles.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
IAM-11	Service Customers Approval for Agreed Privileged Access Roles	Define, implement and evaluate processes and procedures for service customers to participate, where applicable, in the granting of access for agreed, high risk as defined by the organizational risk assessment) privileged access roles.	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	
IAM-12	Unique Identities	Define, implement and evaluate processes, procedures and technical measures that ensure identities' activities are identifiable through uniquely associated IDs.	Functional	Subset Of	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	10	
IAM-13	Strong Authentication	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	8	
IAM-13	Strong Authentication	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Functional	Intersects With	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	8	
IAM-13	Strong Authentication	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.	8	

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
IAM-13	Strong Authentication	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Functional	Intersects With	Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS)	IAC-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	8	
IAM-13	Strong Authentication	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	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/regulate data.	5	
IAM-13	Strong Authentication	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	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.	5	
IAM-13	Strong Authentication	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	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.	3	
IAM-13	Strong Authentication	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	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.	5	
IAM-13	Strong Authentication	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	5	
IAM-14	Credentials Management	Define, implement and evaluate processes, procedures and technical measures for the secure management of authentication credentials, including passwords.	Functional	Intersects With	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.	8	
IAM-14	Credentials Management	Define, implement and evaluate processes, procedures and technical measures for the secure management of authentication credentials, including passwords.	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	
IAM-14	Credentials Management	Define, implement and evaluate processes, procedures and technical measures for the secure management of authentication credentials, including passwords.	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.	3	
IAM-14	Credentials Management	Define, implement and evaluate processes, procedures and technical measures for the secure management of authentication credentials, including passwords.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	3	
IAM-15	Authorization Mechanisms	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	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	
IAM-15	Authorization Mechanisms	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	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	
IAM-15	Authorization Mechanisms	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5	
IAM-15	Authorization Mechanisms	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
IAM-15	Authorization Mechanisms	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Functional	Intersects With	No Embedded Unencrypted Static Authenticators	IAC-10.6	Mechanisms exist to ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys.	5	
IAM-15	Authorization Mechanisms	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
IAM-15	Authorization Mechanisms	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	8	
IPY-01	Interoperability and Portability Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	
IPY-01	Interoperability and Portability Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually, or upon significant changes.	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.	8	
IPY-01	Interoperability and Portability Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	8	
IPY-02	Application Interface Availability	Provide application interface(s) to service customers so that they programmatically retrieve their data to enable interoperability and portability.	Functional	Intersects With	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	8	
IPY-03	Secure Interoperability and Portability Management	Implement cryptographically secure network protocols for the management, import and export of data, according to industry standards.	Functional	Intersects With	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	8	
IPY-03	Secure Interoperability and Portability Management	Implement cryptographically secure network protocols for the management, import and export of data, according to industry standards.	Functional	Intersects With	Data Handling & Portability	CLD-07	Mechanisms exist to ensure cloud providers use secure protocols for the import, export and management of data in cloud-based Technology Assets, Applications and/or Services (TAAS).	8	
IPY-04	Data Portability Contractual Obligations	Agreements must include provisions specifying service customers' access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the service customers d. Data deletion policy	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
IPY-04	Data Portability Contractual Obligations	Agreements must include provisions specifying service customers' access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the service customers d. Data deletion policy	Functional	Intersects With	Adequate Security for Sensitive / Regulated Data in Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive/regulate data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
IPY-04	Data Portability Contractual Obligations	Agreements must include provisions specifying service customers' access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the service customers d. Data deletion policy	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
IPY-04	Data Portability Contractual Obligations	Agreements must include provisions specifying service customers' access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the service customers d. Data deletion policy	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience practices with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAAS).	5	
I65-01	Infrastructure and Virtualization Security Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	
I65-01	Infrastructure and Virtualization Security Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually, or upon significant changes.	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.	8	
I65-01	Infrastructure and Virtualization Security Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually, or upon significant changes.	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	
I65-01	Infrastructure and Virtualization Security Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5	
I65-02	Capacity and Resource Planning	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	Functional	Subset Of	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.	10	
I65-02	Capacity and Resource Planning	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	8	
I65-03	Network Security	Monitor, encrypt and restrict communications between environments, services, and applications to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.	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	
I65-04	OS Hardening and Base Controls	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	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	
I65-05	Production and Non-Production Environments	Separate production and non-production environments to reduce the risk of sensitive production data being used in non-production environments. Production data is sanitized or protected before any authorized non-production use.	Functional	Subset Of	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	10	
I65-06	Segmentation and Segregation	Design, develop, deploy and configure applications and infrastructures such that service customer (tenant) access is appropriately segmented and segregated, monitored and restricted.	Functional	Subset Of	Network Segmentation (macrosegmentation)	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.	10	
I65-07	Migration to Cloud Environments	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.	Functional	Subset Of	Secure Migration Practices	TDA-08.1	Mechanisms exist to ensure secure migration practices purge Technology Assets, Applications and/or Services (TAAS) of test/development/staging data and accounts before it is migrated into a production environment.	10	

FDE #	FDE Name	Focus Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
16S-08	Network Architecture Documentation	Identify and document high-risk environments based on data sensitivity, threat exposure, and business impact.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	8	
16S-08	Network Architecture Documentation	Identify and document high-risk environments based on data sensitivity, threat exposure, and business impact.	Functional	Intersects With	High-Risk Asset Categorization	AST-31.2	Mechanisms exist to categorize a system and/or service as "High Risk" if it poses a significant risk of harm to an individual's: (1) Health; (2) Safety; and/or (3) Fundamental human rights.	8	
16S-08	Network Architecture Documentation	Identify and document high-risk environments based on data sensitivity, threat exposure, and business impact.	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.	5	
16S-09	Network Defense	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	Functional	Subset Of	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.	10	
LOG-01	Logging and Monitoring Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	
LOG-01	Logging and Monitoring Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
LOG-01	Logging and Monitoring Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	8	
LOG-02	Audit Logs Protection	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	Functional	Subset Of	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	10	
LOG-03	Security Monitoring and Alerting	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.	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.	8	
LOG-03	Security Monitoring and Alerting	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from critical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	8	
LOG-03	Security Monitoring and Alerting	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.	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	
LOG-04	Audit Logs Access and Accountability	Restrict audit log access to authorized identities and maintain records of that access.	Functional	Intersects With	Access by Subset of Privileged Users	MON-08.2	Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.	8	
LOG-04	Audit Logs Access and Accountability	Restrict audit log access to authorized identities and maintain records of that access.	Functional	Intersects With	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	8	
LOG-05	Audit Logs Monitoring and Response	Implement and maintain capabilities to correlate and monitor security audit logs for the detection of suspicious or anomalous activity that deviates from typical or expected behavior and follow a defined process to review and take appropriate and timely actions on detected anomalies.	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	
LOG-06	Clock Synchronization	Use a reliable time source across all relevant information processing systems.	Functional	Equal	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	10	
LOG-07	Logging Scope	Establish, document and implement which information metadata system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment, and as per relevant regulatory requirements.	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5	
LOG-07	Logging Scope	Establish, document and implement which information metadata system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment, and as per relevant regulatory requirements.	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
LOG-08	Audit Logs Sanitization	Define, implement and evaluate technical measures for service customers to detect and scrub or tokenize sensitive data from logs to prevent unauthorized exposure, as per applicable laws and regulations.	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.	5	
LOG-09	Log Records	Generate audit records containing relevant security information.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	8	
LOG-10	Audit Records Protection	Protect audit records from unauthorized access, modification, and deletion.	Functional	Subset Of	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	10	
LOG-11	Encryption Monitoring and Reporting	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
LOG-11	Encryption Monitoring and Reporting	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5	
LOG-11	Encryption Monitoring and Reporting	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
LOG-12	Transaction/Activity Logging	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
LOG-13	Access Control Logs	Monitor and log physical access using an auditable access control system.	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	
LOG-14	Failures and Anomalies Reporting	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.	Functional	Intersects With	Anomalous Behavior	MON-16	Automated mechanisms exist to identify and alert on indicators of anomalous behavior that could indicate account compromise or other malicious activities.	5	
LOG-14	Failures and Anomalies Reporting	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	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.	5	
LOG-14	Failures and Anomalies Reporting	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.	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	
LOG-14	Failures and Anomalies Reporting	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.	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.	5	
SEF-01	Security Incident Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	
SEF-01	Security Incident Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
SEF-01	Security Incident Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	
SEF-02	Service Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	
SEF-02	Service Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
SEF-02	Service Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	8	
SEF-03	Incident Response Plans	Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to a communication strategy for notifying relevant internal departments, impacted service customers, and other business critical relationships (such as supply-chain) that may be impacted.	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	
SEF-03	Incident Response Plans	Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to a communication strategy for notifying relevant internal departments, impacted service customers, and other business critical relationships (such as supply-chain) that may be impacted.	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	
SEF-04	Incident Response Testing	Exercise the incident response plans at planned intervals or upon significant changes.	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	
SEF-05	Incident Response Metrics	Establish, monitor and report information security incident metrics.	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCR) measures of performance.	10	
SEF-06	Event Triage Processes	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related 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	

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
SEF-07	Incident Management and Response	Define, implement and evaluate processes, procedures and technical measures for timely and effective response to security incidents in accordance with incident categories and severity levels. Review, update, and test processes and procedures at least annually.	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	
SEF-07	Incident Management and Response	Define, implement and evaluate processes, procedures and technical measures for timely and effective response to security incidents in accordance with incident categories and severity levels. Review, update, and test processes and procedures at least annually.	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	
SEF-08	Security Breach Notification	Define and implement processes, procedures and technical measures for security breach notifications. Report material security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	Functional	Intersects With	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	8	
SEF-08	Security Breach Notification	Define and implement processes, procedures and technical measures for security breach notifications. Report material security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	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	
SEF-08	Security Breach Notification	Define and implement processes, procedures and technical measures for security breach notifications. Report material security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	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	
SEF-09	Incident Records Management	Establish and maintain a secure repository of security incident records. Regularly review the incident records to identify patterns, root causes, and systemic vulnerabilities, and implement relevant corrective measures.	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	
SEF-10	Points of Contact Maintenance	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities. Review and update the points of contact at least annually.	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	8	
STA-01	Supply Chain Risk Management Policies and Procedures	Establish, document, approve, communicate, apply, evaluate, and maintain policies and procedures for supply chain risk management. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	
STA-01	Supply Chain Risk Management Policies and Procedures	Establish, document, approve, communicate, apply, evaluate, and maintain policies and procedures for supply chain risk management. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
STA-01	Supply Chain Risk Management Policies and Procedures	Establish, document, approve, communicate, apply, evaluate, and maintain policies and procedures for supply chain risk management. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	8	
STA-02	SSRM Policy and Procedures	Establish, document, approve, communicate, apply, evaluate, and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASC) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	8	
STA-03	SSRM Supply Chain	Apply, document, implement and manage the SSRM throughout the supply chain.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASC) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	8	
STA-04	SSRM Guidance	Provide SSRM Guidance to the service customers detailing information about the SSRM applicability throughout the supply chain.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
STA-04	SSRM Guidance	Provide SSRM Guidance to the service customers detailing information about the SSRM applicability throughout the supply chain.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASC) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	8	
STA-05	SSRM Control Ownership	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASC) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	8	
STA-06	SSRM Documentation Review	Review and validate the SSRM documentation.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASC) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	8	
STA-07	SSRM Control Implementation	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASC) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	8	
STA-08	Supply Chain Inventory	Develop and maintain an inventory of all supply chain relationships.	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	
STA-09	Service Bill of Material (SBOM)	Define, implement, and enforce a process for establishing a Bill of Material for the service supply chain. Review and update the Bill of Material at least annually or upon significant changes.	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	3	
STA-10	Supply Chain Risk Management	Periodically review risk factors associated with supply chain relationships.	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.	8	
STA-10	Supply Chain Risk Management	Periodically review risk factors associated with supply chain relationships.	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	8	
STA-11	Primary Service and Contractual Agreement	Service agreements must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy • Operational Resilience	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	
STA-11	Primary Service and Contractual Agreement	Service agreements must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy • Operational Resilience	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	8	
STA-12	Supply Chain Agreement Review	Review supply chain agreements at least annually or upon significant changes.	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.	8	
STA-13	Supply Chain Compliance Assessment	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.	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.	8	
STA-14	Supply Chain Service Agreement Compliance	Implement policies requiring all service providers throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.	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.	8	
STA-15	Supply Chain Governance Review	Review the organization's service providers' IT governance policies and procedures at least annually or upon significant changes.	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.	8	
STA-16	Supply Chain Data Security Assessment	Define and implement a process for conducting risk-based security assessments of the supply chain.	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	
TMV-01	Threat and Vulnerability Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities and threats, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	
TMV-01	Threat and Vulnerability Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities and threats, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
TMV-01	Threat and Vulnerability Management Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities and threats, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Vulnerability & Patch Management Program (VPM)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	8	
TMV-02	Malware and Malicious Instructions Protection Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware and malicious instructions. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	
TMV-02	Malware and Malicious Instructions Protection Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware and malicious instructions. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	

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
TVM-02	Malware and Malicious Instructions Protection Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware and malicious instructions. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	8	
TVM-03	Vulnerability Identification	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	8	
TVM-03	Vulnerability Identification	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	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	
TVM-04	Threat Analysis and Modeling	Define, implement, and evaluate a threat analysis process and procedures to identify, assess, and review the threat landscape for cloud systems. Build threat models according to industry best practices to inform the risk mitigation strategy.	Functional	Intersects With	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.	8	
TVM-04	Threat Analysis and Modeling	Define, implement, and evaluate a threat analysis process and procedures to identify, assess, and review the threat landscape for cloud systems. Build threat models according to industry best practices to inform the risk mitigation strategy.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRPR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
TVM-04	Threat Analysis and Modeling	Define, implement, and evaluate a threat analysis process and procedures to identify, assess, and review the threat landscape for cloud systems. Build threat models according to industry best practices to inform the risk mitigation strategy.	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	8	
TVM-05	Detection Updates	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	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	
TVM-05	Detection Updates	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	8	
TVM-06	External Library Vulnerabilities	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	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	
TVM-06	External Library Vulnerabilities	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	8	
TVM-07	Penetration Testing	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	Functional	Subset Of	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	10	
TVM-08	Vulnerability Remediation Schedule	Define, implement and evaluate processes, procedures and technical measures based on identified risks to support scheduled and emergency responses to vulnerability identification.	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	
TVM-09	Vulnerability Prioritization	Use a risk-based method for effective prioritization of vulnerability remediation using an industry recognized framework.	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	
TVM-10	Threat Response	Use a risk-based method for the prioritization and mitigation of threats, leveraging an industry-recognized framework to guide threat decision-making and protection measures.	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.	8	
TVM-10	Threat Response	Use a risk-based method for the prioritization and mitigation of threats, leveraging an industry-recognized framework to guide threat decision-making and protection measures.	Functional	Intersects With	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.	8	
TVM-11	Vulnerability Management Reporting	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	
TVM-12	Vulnerability Management Metrics	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRPR) measures of performance.	10	
UEM-01	Endpoint Devices Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	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.	8	
UEM-01	Endpoint Devices Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRPR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
UEM-01	Endpoint Devices Policy and Procedures	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually, or upon significant changes.	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	8	
UEM-02	Application and Service Approval	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	Functional	Intersects With	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.	8	
UEM-03	Compatibility	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
UEM-04	Endpoint Inventory	Maintain an inventory of all endpoints used to store, access and process company data.	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	