Set Theory Relationship Mapping (STRM)



Reference Document: Secure Controls Framework (SCF) version 2024.2

Focal Document URL: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

Focal Document: AICPA 2017 Trust Services Criteria (TSC) with revised Points of Focus - 2022

STRM URL: https://content.securecontrolsframework.com/strm/scf-2024-2-tsc-2017.pdf

Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two concepts are related:

- 1. Syntactic: How similar is the wording that expresses the two concepts? This is a word-for-word analysis of the relationship, not an interpretation of the language.
- 2. Semantic: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
- 3. Functional: How similar are the <u>results</u> of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed

Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two distinct concepts:

- 1. Subset Of
- 2. Intersects With
- 3. Foual
- 4. Superset Of
- 5. No Relationship



Relationship Type #1:

Focal Document Element is a subset of SCF control. In other words, SCF control contains everything that Focal Document Element does and more.

Relationship Type #2: INTERSECTS WITH

SCF control has some overlap with Focal Document Element, but each includes content that the other does not.

Relationship Type #3: EQUAL

SCF control and Focal Document Element are the same, although not necessarily identical.

Relationship Type #4: SUPERSET OF

Focal Document Element is a superset of SCF control. In other words, Focal Document Element contains everything that SCF control does and more.

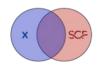
Relationship Type #5:

SCF control and Focal Document Element are unrelated; their content does not overlap.



SUBSET OF

Relative Relationship Strength (control versus control)



INTERSECTS WITH

Relative Relationship Strength (control versus control)



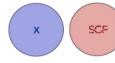
EQUAL

Relative Relationship Strength (control versus control)



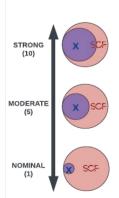
SUPERSET OF

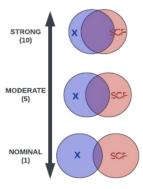
Relative Relationship Strength (control versus control)

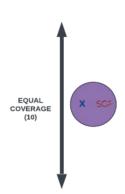


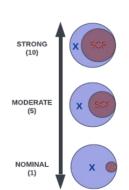
NO RELATIONSHIP

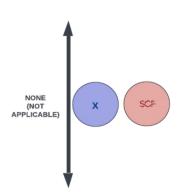
Relative Relationship Strength (control versus control)













FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		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	
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (Infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Functional	intersects with	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of systems that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	
		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.	5	
		Functional	intersects with	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5	
A1.1-POF1	Measures Current Usage	Functional	subset of	Performance Monitoring	CAP-04	Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical systems, applications and services.	10	
A1.1-POF2	Forecasts Capacity	Functional	equal	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.	10	
A1.1-POF3	Makes Changes Based on Forecasts	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	
		Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
		Functional	intersects with	Alternate Storage Site	BCD-08	Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.	5	
		Functional	intersects with	Separation from Primary Site	BCD-08.1	Mechanisms exist to separate the alternate storage site from the primary storage site to reduce susceptibility to similar threats.	5	
		Functional	intersects with	Accessibility	BCD-08.2	Mechanisms exist to identify and mitigate potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.	5	
		Functional	intersects with	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	5	
		Functional	intersects with	Separation from Primary Site	BCD-09.1	Mechanisms exist to separate the alternate processing site from the primary processing site to reduce susceptibility to similar threats.	5	
		Functional	intersects with	Accessibility	BCD-09.2	Mechanisms exist to identify and mitigate potential accessibility problems to the alternate processing site and possible mitigation actions, in the event of an area-wide disruption or disaster.	5	
		Functional	intersects with	Alternate Site Priority of Service	BCD-09.3	Mechanisms exist to address priority-of-service provisions in alternate processing and storage sites that support availability requirements, including Recovery Time Objectives (RTOs).	5	
		Functional	intersects with	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.	5	
		Functional	intersects with	Telecommunications Priority of Service Provisions	BCD-10.1	Mechanisms exist to formalize primary and alternate telecommunications service agreements contain priority-of-service provisions that support availability requirements, including Recovery Time Objectives (RTOs).	5	
		Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
		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.	5	
		Functional	intersects with	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	5	
		Functional	intersects with	Information System Imaging	BCD-11.3	Mechanisms exist to reimage assets from configuration-controlled and integrity- protected images that represent a secure, operational state.	5	
		Functional	intersects with	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
		Functional	intersects with	Information System Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of systems to a known state after a disruption, compromise or failure.	5	
		Functional	intersects with	Transaction Recovery	BCD-12.1	Mechanisms exist to utilize specialized backup mechanisms that will allow transaction recovery for transaction-based applications and services in accordance with Recovery Point Objectives (RPOs).	5	
		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 systems, applications and/or services.	5	
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	Functional	intersects with	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
		Functional	intersects with	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	5	
		Functional	intersects with	Automatic Voltage Controls	PES-07.1	Facility security mechanisms exist to utilize automatic voltage controls for critical system components.	5	
		Functional	intersects with	Emergency Shutoff	PES-07.2	Facility security mechanisms exist to shut off power in emergency situations by: • Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and • Protecting emergency power shutoff capability from unauthorized activation.	5	
		Functional	intersects with	Emergency Power		Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the	5	
		Functional	intersects with	Emergency Lighting		primary power source. 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	5	
		Functional	intersects with	Water Damage Protection	PES-07.5	exits and evacuation routes within the facility. Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and	5	
		Functional	intersects with	Fire Protection	PES-08	known to key personnel. Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	5	
		Functional	intersects with	Fire Detection Devices	PES-08.1	Facility security mechanisms exist to utilize and maintain fire detection devices/systems that activate automatically and notify organizational personnel and emergency	5	
		Functional	intersects with	Fire Suppression Devices	PES-08.2	responders in the event of a fire. Facility security mechanisms exist to utilize fire suppression devices/systems that provide automatic notification of any activation to organizational personnel and	5	
		Functional	intersects with	Temperature & Humidity Controls	PES-09	emergency responders. Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	5	
		Functional	intersects with	Monitoring with Alarms / Notifications	PES-09.1	Facility security mechanisms exist to trigger an alarm or notification of temperature and humidity changes that be potentially harmful to personnel or equipment.	5	
		Functional	intersects with	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized	5	
		Functional	intersects with	Alternate Work Site	PES-11	access. Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	5	
		Functional	intersects with	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize	5	
		Functional	intersects with	Information Leakage Due To Electromagnetic Signals	PES-13	the opportunity for unauthorized access. Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.	5	
		Functional	intersects with	Emanations Electromagnetic Pulse (EMP) Protection	PES-15	Physical security mechanisms exist to employ safeguards against Electromagnetic Pulse (EMP) damage for systems and system components.	5	
		Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
		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,	5	
		Functional	intersects with	Business Continuity Management System	BCD-01	modification or destruction of the organization's systems and data. Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or	5	
				(BCMS) Physical & Environmental		Business Continuity & Disaster Recovery (BC/DR) playbooks). Mechanisms exist to facilitate the operation of physical and environmental protection		
A1.2-POF1	Identifies Environmental Threats	Functional	intersects with	Protections	PES-01	controls.	5	



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
		Functional	equal	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	10	
		Functional	intersects with	Business Continuity Management System	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or	5	
				(BCMS) Physical & Environmental		Business Continuity & Disaster Recovery (BC/DR) playbooks). Mechanisms exist to facilitate the operation of physical and environmental protection	_	
A1.2-POF2	Designs Detection Measures	Functional	intersects with	Protections Temperature & Humidity	PES-01 PES-09	controls. Facility security mechanisms exist to maintain and monitor temperature and humidity	5	
		Functional	intersects with	Controls Monitoring with Alarms /	PES-09.1	levels within the facility. Facility security mechanisms exist to trigger an alarm or notification of temperature and humidity changes that be potentially harmful to personnel or equipment.	5	
A1.2-POF3	Implements and Maintains Environmental Protection Mechanisms	Functional	intersects with	Notifications Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
		Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
		Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
A1.2-POF4	Implements Alerts to Analyze Anomalies	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
		Functional	intersects with	Temperature & Humidity Controls Monitoring with Alarms (PES-09	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility. Facility security mechanisms exist to trigger an alarm or notification of temperature and	5	
		Functional	intersects with	Monitoring with Alarms / Notifications	PES-09.1	humidity changes that be potentially harmful to personnel or equipment. Mechanisms exist to facilitate the implementation of contingency planning controls to	5	
		Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	mechanisms east to attended the impresentation to competing paraming controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks). Mechanisms exist to implement and govern processes and documentation to facilitate	5	
44.3.8055		Functional	subset of	Incident Response Operations	IRO-01	an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
A1.2-POF5	Responds to Environmental Threat Events	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
		Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
A1.2-POF6	Communicates and Reviews Detected Environmental Threat Events	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
		Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
		Functional Functional	subset of intersects with	Data Protection Sensitive / Regulated Data	DCH-01 DCH-01.2	Mechanisms exist to facilitate the implementation of data protection controls. Mechanisms exist to protect sensitive/regulated data wherever it is stored.	10	
		Functional	intersects with	Protection	DCH-01.2	Mechanisms exist to create recurring backups of data, software and/or system images,	,	
A1.2-POF7	Determines Data Requiring Backup	Functional	intersects with	Data Backups Physical & Environmental	BCD-11	as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Mechanisms exist to facilitate the operation of physical and environmental protection	5	
		Functional	intersects with	Protections	PES-01	controls. Mechanisms exist to create recurring backups of data, software and/or system images,	5	
A1.2-POF8	Performs Data Backup	Functional	intersects with	Data Backups	BCD-11	as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Mechanisms exist to establish an alternate storage site that includes both the assets	5	
		Functional	intersects with	Alternate Storage Site	BCD-08	and necessary agreements to permit the storage and recovery of system backup information. Metabolisms switch to choose backup copies of critical coffusion and other copyright solated.	5	
A1.2-POF9	Addresses Offsite Storage	Functional	intersects with	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up. Mechanisms exist to transfer backup data to the alternate storage site at a rate that is	5	
		Functional	intersects with	Transfer to Alternate Storage Site	BCD-11.6	capable of meeting both Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
		Functional	intersects with	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
A1.2-POF10	Implements Alternate Processing Infrastructure	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
		Functional	subset of	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	10	
		Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
A1.2-POF11	Considers Data Recoverability	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: - Assumptions effecting risk assessments, risk response and risk monitoring; - Constraints affecting risk assessments, risk response and risk monitoring; - Constraints affecting risk assessments, risk response and risk monitoring; - The organizational risk tolerance; and - Priorittes, benefits and trade-offs considered by the organization for managing risk.	5	
		Functional	intersects with	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
		Functional	intersects with	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
		Functional	intersects with	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5	
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Functional	intersects with	Simulated Events	BCD-03.1	Mechanisms exist to incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations. Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's	5	
		Functional	intersects with	Contingency Plan Testing & Exercises		effectiveness and the organization's readiness to execute the plan. Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's	5	
A1.3-POF1	Implements Business Continuity Plan Testing	Functional	equal	Contingency Plan Testing & Exercises Contingency Plan Testing &	BCD-04	effectiveness and the organization's readiness to execute the plan. Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's	10	
A1.3-POF2	Tests Integrity and Completeness of Backup Data	Functional	intersects with	Exercises Testing for Reliability &	BCD-04 BCD-11.1	effectiveness and the organization's readiness to execute the plan. Mechanisms exist to routinely test backups that verify the reliability of the backup	5	
		Functional	intersects with	Integrity Test Restoration Using Sampling	BCD-11.5	process, as well as the integrity and availability of the data. Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	5	
		Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related	Functional	intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements. Mechanisms exist to control and restrict access to digital and non-digital media to	5	
C1.1-POF1	Defines and identifies Confidential information	Functional	intersects with	Media Access Network Diagrams & Data Flow Diagrams (DFDs)	DCH-03 AST-04	authorized individuals. Mechanisms exist to maintain network architecture diagrams that: - Contain sufficient detail to assess the security of the network's architecture; - Reflect the current architecture of the network environment; and	5	
CLITOFI		Functional	intersects with	Sensitive Data Inventories	DCH-06.2	Document all sensitive/regulated data flows. Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5	
C1.1-P0F2	Retains Confidential Information	Functional	subset of	Data Protection Sensitive / Regulated Data	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls. Mechanisms exist to protect sensitive/regulated data wherever it is stored.	10	
		Functional	intersects with	Sensitive / Regulated Data Protection	DCH-01.2	regulated data wherever it is stored.	5	



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF N	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		Functional	subset of	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	(optional) 10	
C1.1-POF3	Protects Confidential Information From Destruction	Functional	intersects with	Personal Data Retention &	PRI-05	Mechanisms exist to: • 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; • Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of	5	
				Disposal		storage, and • Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).		
		Functional	subset of intersects with	Information Disposal Event Log Retention	MON-10	Mechanisms exist to securely dispose of, destroy or erase information. Mechanisms exist to retain event logs or 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.	5	
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.					Mechanisms exist to: Retain Personal Data (PD), including metadata, for an organization-defined time		
		Functional	intersects with	Personal Data Retention & Disposal	PRI-05	period to fulfill the purpose(s) identified in the notice or as required by law; - Dispose of, destroys, erases, angle, anonymites the PD, regardless of the method of storage; and - Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
		Functional	subset of	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	10	
C1.2-POF1	Identifies Confidential Information for Destruction	Functional	intersects with	Personal Data Retention & Disposal	PRI-05	Mechanisms exist to: **Retain Personal stat (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; **Dispose of, destroys, erases, and/or anonymites the PD, regardless of the method of storage; and **Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
		Functional	intersects with	Secure Disposal, Destruction or Re-Use of	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being	5	
		Functional	intersects with	Equipment Physical Media Disposal	DCH-08	recovered from these components. Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
		Functional	intersects with	System Media Sanitization	DCH-09	normal procedures. 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. Mechanisms exist to securely dispose of, destroy or erase information.	5	
C1.2-POF2	Destroys Confidential Information	Functional	intersects with	Information Disposal	DCH-21	Mechanisms exist to:	5	
		Functional	intersects with	Personal Data Retention & Disposal	PRI-05	 Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or a required by law; Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records). 	5	
		Functional	subset of	Cybersecurity & Data Protection Governance	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
		Functional	intersects with	Program Cybersecurity & Data Protection Controls	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
CC1.1	COSO Principle 1	Functional	intersects with	Oversight Assigned Cybersecurity & Data Protection 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 cybersecurity & data protection program.	5	
		Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
		Functional	intersects with	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity & data privacy principles in their daily work.	5	
		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. Mechanisms exist to conduct employee misconduct investigations when there is	5	
		Functional	intersects with	Workplace Investigations Cybersecurity & Data	HRS-07.1	mechanisms exist to facilitate the implementation of cybersecurity & data protection Mechanisms exist to facilitate the implementation of cybersecurity & data protection	5	
CC1.1-POF1	Sets the Tone at the Top	Functional	subset of	Protection Governance Program Business As Usual (BAU)	GOV-01	governance controls. Mechanisms exist to incorporate cybersecurity & data privacy principles into Business As Usual (BAU) practices through executive leadership involvement.	10	
		Functional	intersects with	Secure Practices Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.1-POF2	Establishes Standards of Conduct	Functional	equal	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.	10	
		Functional	subset of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	10	
		Functional	subset of	Cybersecurity & Data Protection Controls	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	10	
CC1.1-POF3	Evaluates Adherence to Standards of Conduct	Functional	intersects with	Oversight Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	5	
		Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
		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	
CC1.1-POF4	Addresses Deviations in a Timely Manner	Functional	intersects with	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
		Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
		Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
		Functional	intersects with	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
CC1.1-POF5	Considers Contractors and Vendor Employees in Demonstrating Its Commitment	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
		Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
		Functional	intersects with	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
		Functional	intersects with	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
		Functional	subset of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	10	
		Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
CC1.2	COSO Principle 2	Functional	intersects with	Key Performance Indicators (KPIs)	GOV-05.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring and trend analysis of the cybersecurity & data privacy program.	5	
CC1.2		Functional	intersects with	Key Risk Indicators (KRIs)	GOV-05.2	Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the cybersecurity & data privacy program.	5	
		Functional	intersects with	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
		Functional	intersects with	Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.	5	
		Functional	intersects with	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
			I .	1	1	I.	1	L



## 1870년 전 1	FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
# 1			Functional	subset of			through a steering committee or advisory board, comprised of key cybersecurity, data	10	
Heater Properties of the control o			Functional	intersects with	Publishing Cybersecurity & Data Protection	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data	5	
Health Properties of the control of			Functional	intersects with	Stakeholder Accountability		individuals are empowered, responsible and trained for mapping, measuring and	5	
Heater septimate for the septimate of t			Functional	intersects with	Authoritative Chain of	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	5	
Heater segments of the composition of the composit	CC1.2-POF1	Establishes Oversight Responsibilities	Functional	intersects with	Defining Business Context		Mechanisms exist to define the context of its business model and document the mission of the organization.	5	
Heater the second secon			Functional	intersects with	Data Governance		standards and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual	5	
Heater the section of			Functional	intersects with		HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
1			Functional	intersects with	Position Categorization	HRS-02	all positions and establishing screening criteria for individuals filling those positions.	5	
1					Steering Committee &		Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data		
Marie					Human Resources Security			5	
1	CC1 2-POE2	Anniles Balavant Evnertice							
1	CC1.2 1 012	reparted to the conference							
1					Competency Requirements for Security-Related				
Marie Mari									
Marie Mari	CC1.2-POF3	Operates Independently			Program Oversight		privacy and business executives, which meets formally and on a regular basis.		
	CC1.2 1 013	орение инсерситенту			Management	HK3-01	Mechanisms exist to manage personnel security risk by assigning a risk designation to		
Part							Mechanisms exist to coordinate cybersecurity, data protection and business alignment		
March Marc			Functional	intersects with	Program Oversight		privacy and business executives, which meets formally and on a regular basis.	5	
Part	CC1.2-POF4	Supplements Board Expertise	Functional	intersects with		HRS-01		5	
Part			Functional	intersects with			all positions and establishing screening criteria for individuals filling those positions.	5	
Part			Functional	intersects with	for Security-Related Positions	HRS-03.2	individuals who have the necessary skill set.	5	
No. Control			Functional	intersects with	Data Protection	GOV-04	resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
Part			Functional	intersects with		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 data and technology-related risks.	5	
			Functional	intersects with			communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
	CC1.3	COSO Principle 3	Functional	intersects with		HRS-03	Mechanisms exist to ensure that all security-related positions are staffed by qualified	5	
Punctional Pun			Functional	intersects with	for Security-Related	HRS-03.2		5	
CCL 3 POTE			Functional	intersects with	Business Process Definition		data privacy that determines: The resulting risk to organizational operations, assets, individuals and other organizations; and Information protection needs arising from the defined business processes and revises	5	
Proctional Interacts with Second Process and Process with Second Process with			Functional	intersects with		COV 01 1	through a steering committee or advisory board, comprised of key cybersecurity, data	5	
Punctional Interacts with Authoritative Chain of Command with Care lives	CC1.3-POF1	Considers All Structures of the Entity	Functional	intersects with			individuals are empowered, responsible and trained for mapping, measuring and	5	
Functional Intersects with Solakholder Accountability (Intersect of the Society of the Soc			Functional	intersects with			Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing	5	
Functional intersects with Command Functional intersects with Command Functional intersects with Selecting Committee & Program Overlage Functional intersects with Selecting Committee & Selecting Committee or Selec			Functional	intersects with	Stakeholder Accountability	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	5	
Functional Intersects with Seering Committee & Program Oversight CVV-13. Selection Committee & Program Oversight CVV-13. Selection Committee & Program Oversight CVV-13.	CC1.3-POF2	Establishes Reporting Lines	Functional	intersects with			Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing	5	
Functional intersects with Sourcement Succession of Succession (Application of Application of Ap			Functional	intersects with		COV 01 4	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data	5	
Predictional intersects with Command Com			Functional	intersects with		GOV-04.1	individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	
Functional intersects with Punctional intersects with Punctional intersects with Intersects with Punctional intersects with In	CC1.3-POF3	Defines, Assigns, and Limits Authorities and Responsibilities	Functional	intersects with	Authoritative Chain of Command		communication to remove ambiguity from individuals and teams related to managing	5	
Functional Intersects with Supportive, Crossilled & Informed (RACC) Matrix, or similar documentation, to delineate informed (RACC) matrix, or similar docume			Functional	intersects with	Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.	5	
Functional intersects with Functional intersects with COUNTIAN COU			Functional	intersects with	Supportive, Consulted &		Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
Functional Intersects with Authoritative Chain of Command Command Command GOV-0.2 GOV-0.2 Gommunication to remove ambiguity from individuals and teams related to managing 5 Mechanisms exist to document and maintain a Responsibilities for all personnel. Functional Intersects with Responsibilities Functional Intersects with Punctional Intersects with Intersects			Functional	intersects with			Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	
Functional Intersects with Roles & Responsibilities HRS-03 Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Martin, or similar documentation, to delineate saigment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ISPA). Stakeholder Accountability Structure on the Command of Command intersects with Authoritative Chain of Command of			Functional	intersects with		GOV-04.2	communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
Functional intersects with int	CC1.3-P0F4	Authorities and Responsibilities	Functional	intersects with	Roles & Responsibilities	HRS-03		5	
Functional intersects with Stakeholder Accountability Structure GOV-0.1 individuals are empowered, responsible and trained for mapping, measuring and 5 managing data and trenology-related risks. Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.			Functional	intersects with	Supportive, Consulted &	TPM-05.4	Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
Functional intersects with Authoritative Chain of Command GOV-04.2 data and technology-related risks.			Functional	intersects with		GOV-04.1	individuals are empowered, responsible and trained for mapping, measuring and	5	
CCI 3-POFS Considers Interactions With External Parties When Establishing Structures, Reporting Lines, Authorities, and	CC1 3-POF5	Considers Interactions With External Parties When Establishing Structures, Reporting Lines, Authorities, and	Functional	intersects with		GOV-04.2	communication to remove ambiguity from individuals and teams related to managing	5	



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF II	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
 	Responsibilities	Functional	intersects with	Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.	(optional) 5	
		Functional	intersects with	Responsible, Accountable, Supportive, Consulted &	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for Optensecurity & data privacy controls between internal stakeholders and	5	
		Functional	intersects with	Informed (RASCI) Matrix Stakeholder Accountability	GOV-04.1	External Service Providers (ESPs). Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and	5	
		Functional	intersects with	Structure Authoritative Chain of	GOV-04.2	managing data and technology-related risks. Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing	5	
CC1.3-POF6	Establishes Structures, Reporting Lines, and Authorities to Support Compliance With Legal and Contractual Privacy	Functional	intersects with	Command Human Resources Security	HRS-01	data and technology-related risks. Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.5+010	Requirements			Management		Mechanisms exist to facilitate the implementation and operation of data privacy		
		Functional	intersects with	Data Privacy Program	PRI-01	controls. Mechanisms exist to ensure that the interests of external service providers are	5	
		Functional	intersects with subset of	Conflict of Interests Human Resources Security	TPM-04.3 HRS-01	consistent with and reflect organizational interests. Mechanisms exist to facilitate the implementation of personnel security controls.	5	
		Functional	intersects with	Management Cybersecurity & Data Privacy Resource	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity & data privacy programs and	5	
		Functional	intersects with	Management Allocation of Resources	PRM-03	document all exceptions to this requirement. Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects /	5	
CC1.4	COSO Principle 4	Functional	intersects with	Cybersecurity & Data	SAT-01	initiatives. Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
				Privacy-Minded Workforce Continuing Professional Education (CPE) -		Mechanisms exist to ensure cybersecurity & data privacy personnel receive Continuing Professional Education (CPE) training to maintain currency and proficiency with industry.		
		Functional	intersects with	Cybersecurity & Data Privacy Personnel	SAT-03.7	recognized secure practices that are pertinent to their assigned roles and responsibilities.	5	
CC1.4-POF1	Establishes Policies and Practices	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
		Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
		Functional	intersects with	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	5	
		Europhia 1	intersects with	AI & Autonomous Technologies Stakeholder	AAT-13.1	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related operator and practitioner proficiency requirements for Artificial	5	
		Functional	miersecis with	Competencies	MAI-15.1	Intelligence (AI) and Autonomous Technologies (AAT) are defined, assessed and documented. Mechanisms exist to facilitate the implementation of personnel security controls.	3	
		Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to identify newly onboarded personnel for enhanced monitoring	5	
CC1.4-POF2	Evaluates Competence and Addresses Shortcomings	Functional	intersects with	Probationary Periods	HRS-02.2	during their probationary period.	5	
		Functional	intersects with	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
		Functional	intersects with	Identify Critical Skills & Gaps	HRS-13	Mechanisms exist to evaluate the critical cybersecurity & data privacy skills needed to support the organization's mission and identify gaps that exist.	5	
		Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
		Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
		Functional	intersects with	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
		Functional	intersects with	AI & Autonomous Technologies Stakeholder Diversity	AAT-13	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholder competencies, skills and capacities incorporate demographic diversity, broad domain and user experience expertise.	5	
		Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
		Functional	intersects with	Probationary Periods	HRS-02.2	Mechanisms exist to identify newly onboarded personnel for enhanced monitoring during their probationary period.	5	
CC1.4-POF3	Attracts, Develops, and Retains Individuals	Functional	intersects with	Identify Critical Skills & Gaps	HRS-13	Mechanisms exist to evaluate the critical cybersecurity & data privacy skills needed to support the organization's mission and identify gaps that exist.	5	
		Functional	intersects with	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
		Functional	intersects with	Continuing Professional Education (CPE) -	SAT-03.7	Mechanisms exist to ensure cybersecurity & data privacy personnel receive Continuing Professional Education (CPE) training to maintain currency and proficiency with industry	5	
		B		Cybersecurity & Data Privacy Personnel	****	recognized secure practices that are pertinent to their assigned roles and responsibilities. Mechanisms exist to facilitate the implementation of third-party management controls.	_	
		Functional	intersects with	Third-Party Management Review of Third-Party	TPM-01	Mechanisms exist to monitor, regularly review and audit External Service Providers	5	
		Functional	intersects with	Services Identify Critical Skills &	TPM-08 HRS-13	(ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls. Mechanisms exist to evaluate the critical cybersecurity & data privacy skills needed to	5	
CC1.4-POF4	Plans and Prepares for Succession	Functional	intersects with	Gaps Perform Succession Planning	HRS-13.4	support the organization's mission and identify gaps that exist. Mechanisms exist to perform succession planning for vital cybersecurity & data privacy roles.	5	
CC1.4-POF5	Considers the Background of Individuals	Functional	equal	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access. Mechanisms exist to define cybersecurity responsibilities for all personnel.	10	
CC1.4-POF6	Considers the Technical Competency of Individuals	Functional	intersects with	Roles & Responsibilities Competency Requirements	HRS-03	Mechanisms exist to ensure that all security-related positions are staffed by qualified	5	
		Functional	equal	for Security-Related Positions	HRS-03.2	Individuals who have the necessary skill set.	10	
		Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
CC1.4-POF7	Provides Training to Maintain Technical Competencies	Functional	intersects with	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: - Before authoring access to the system or performing assigned duties; - When required by system changes; and - Annually thereafter.	5	
CC1.4-POF/	riowies iraning (O Maintain Technical Competencies	Functional	intersects with	Continuing Professional Education (CPE) - Cybersecurity & Data Privacy Personnel	SAT-03.7	Mechanisms exist to ensure cybersecurity & data privacy personnel receive Continuing Professional Education (CPE) training to maintain currency and proficiency with industry- recognized secure practices that are pertinent to their assigned roles and responsibilities.	5	
		Functional	intersects with	Continuing Professional Education (CPE) - DevOps Personnel	SAT-03.8	Mechanisms exist to ensure application development and operations (DevOps) personnel receive Continuing Professional Education (CPE) training on Secure Software Development Practices (SSDP) to appropriately address evolving threats.	5	
		Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance. Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to	5	
		Functional	intersects with	Key Performance Indicators (KPIs)	GOV-05.1	assist organizational management in performance monitoring and trend analysis of the cybersecurity & data privacy program.	5	
		Functional	intersects with	Key Risk Indicators (KRIs)	GOV-05.2	Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the cybersecurity & data privacy program.	5	
		Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. Mechanisms exist to document and review instances of non-compliance with statutory,	5	
		Functional	intersects with	Non-Compliance Oversight	CPL-01.1	regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	



CC1.5 CC								
CC1.5 CC		Functional	intersects with	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
CC1.5 CC		Functional	intersects with	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	5	
	OSO Principle 5	Functional	intersects with	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.	5	
		Functional	intersects with	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
		Functional	intersects with	Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.	5	
		Functional	intersects with	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to systems and facilities upon personnel reassignment or transfer, in a timely manner.	5	
		Functional	intersects with	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
		Functional	intersects with	Asset Collection	HRS-09.1	Mechanisms exist to retrieve organization-owned assets upon termination of an individual's employment. Mechanisms exist to expedite the process of removing "high risk" individual's access to	5	
		Functional	intersects with	High-Risk Terminations	HRS-09.2	systems and applications upon termination, as determined by management. Mechanisms exist to govern former employee behavior by notifying terminated	5	
		Functional	intersects with	Post-Employment Requirements	HRS-09.3	individuals of applicable, legally binding post-employment requirements for the protection of organizational information.	5	
		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 data and technology-related risks. Mechanisms exist to establish an authoritative chain of command with clear lines of	5	
CC1.5-POF1 En	nforces Accountability Through Structures, Authorities, and Responsibilities	Functional	intersects with	Authoritative Chain of Command	GOV-04.2	communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
		Functional	intersects with	Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.	5	
		Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
CC1.5-POF2 Es	stablishes Performance Measures, Incentives, and Rewards	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
CC1.5-POF3 Ev	valuates Performance Measures, Incentives, and Rewards for Ongoing Relevance	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.5-POF4 Co	onsiders Excessive Pressures	Functional	subset of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	10	
		Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
		Functional	subset of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	10	
CC1.5-POF5 Ev	usbuste Bufarangers and Bounder or Ricialities Individuals	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
CCI.SPOPS EV	valuates Performance and Rewards or Disciplines Individuals	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
		Functional	intersects with	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
CC1.5-POF6 Ta	akes Disciplinary Actions	Functional	equal	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	10	
		Functional	intersects with	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: - Contain sufficient detail to assex the security of the network's architecture; - Reflect the current architecture of the network environment; and - Document all sensitive/regulated data flows. Mechanisms exist to facilitate the implementation of data protection controls.	5	
		Functional	intersects with	Data Protection Data Stewardship	DCH-01 DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and	5	
		Functional	intersects with	Data & Asset Classification	DCH-02	communicated. Mechanisms exist to ensure data and assets are categorized in accordance with	5	
CC2.1 CC	OSO Principle 13	Functional	intersects with	Data Quality Operations	DCH-22	applicable statutory, regulatory and contractual requirements. Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information across the information lifecycle.	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management or neurae appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
		Functional	intersects with	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5	
		Functional	intersects with	Operationalizing Cybersecurity & Data	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under	5	
CC2.1-POF1 Ide	Information Requirements	Functional	intersects with	Protection Practices Service Delivery (Business Process Support)	OPS-03	their control. Mcchanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
		Functional	intersects with	Operationalizing Cybersecurity & Data	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under	5	
CC2.1-POF2 Ca	aptures Internal and External Sources of Data	Functional	intersects with	Protection Practices Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	their control. **Contain sufficient detail to assess the security of the network's architecture; **Endient the contain sufficient detail to assess the security of the network's architecture; **Enliest the current architecture of the network environment; and **Document all sensitive regulated data flows.	5	
	-	Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	**Note that the state of the st	5	
		Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
CC2.1-POF3 Pri	rocesses Relevant Data Into Information	Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, editivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
		Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
		Functional	intersects with	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and deidentification of information across the information lifecycle.	5	
CC2.1-POF4 M	taintains Quality Throughout Processing	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF II	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
						Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and	(optional)	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
		Functional	intersects with	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of technology assets where sensitive/regulated data is stored, transmitted or processed.	5	
CC2.1-POF5	Documents Data Flow	Functional	subset of	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: - Contain sufficient detail to assess the security of the network's architecture; - Reflect the current architecture of the network environment; and - Document all sensitive/regulated data flows.	10	
		Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
		Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: *Accurately reflects the current systems, applications and services in use, eleventifies authories ofsolwave products, including business justification details; *b at the level of granularity deemed necessary for tracking and reporting; *binduces organisation defined information deemed necessary to achieve effective property accountability; and *binduces organisation defined information deemed necessary to achieve effective property accountability; and	5	
CC2.1-POF6	Manages Assets	Functional	intersects with	Automated Location Tracking	AST-02.10	Mechanisms exist to track the geographic location of system components.	5	
		Functional	intersects with	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5	
		Functional	intersects with	Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.	5	
		Functional	intersects with	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
		Functional	equal	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	10	
CC2.1-POF7	Classifies Information	Functional	intersects with	Data Reclassification	DCH-11	Mechanisms exist to reclassify data, including associated systems, applications and services, commensurate with the security category and/or classification level of the	5	
CC2.1-PUF/	haddens a mod 1188 001	Functional	intersects with	Asset Scope Classification	AST-04.1	information. Mechanisms exist to determine cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties).	5	
						Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-		
CC2.1-POF8	Uses Information That is Complete and Accurate	Functional	subset of	Data Quality Operations	DCH-22	identification of information across the information lifecycle. Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement	10	
		Functional	intersects with	Asset Governance	AST-01	and manage asset management controls.	5	
		Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: **Accurately reflects the current systems, applications and services in use; **Identifies authorized software products, including business justification details; **Identifies organization details; **Includes organization-defined information deemed necessary to tacking and reporting; **Includes organization-defined information deemed necessary to achieve effective property accountability; and **Is available for review and audit by designated organizational personnel.	5	
	Manages the Location of Assets	Functional	intersects with	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of technology assets where sensitive/regulated data is stored, transmitted or processed.	5	
		Functional	intersects with	Automated Location Tracking	AST-02.10	Mechanisms exist to track the geographic location of system components.	5	
CC2.1-POF9		Functional	intersects with	Data Storage Location Reviews	BCD-02.4	Mechanisms exist to perform periodic security reviews of storage locations that contain sensitive / regulated data.	5	
		Functional	intersects with	Geolocation Requirements for Processing, Storage and Service Locations		Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
		Functional	intersects with	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.	5	
		Functional	intersects with	Information Location	DCH-24	Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.	5	
		Functional	intersects with	Change Processing & Storage Locations	SEA-14.2	Automated mechanisms exist to change the location of processing and/or storage at random time intervals.	5	
		Functional	intersects with	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	
		Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
		Functional	intersects with	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
		Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
		Functional	intersects with	Key Performance Indicators (KPIs)	GOV-05.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring and trend analysis of the cybersecurity & data privacy program.	5	
		Functional	intersects with	Key Risk Indicators (KRIs)	GOV-05.2	Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the cybersecurity & data privacy program.	5	
		Functional	intersects with	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5	
CC2.2	COSO Principle 14	Functional	intersects with	Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel. Mechanisms exist to facilitate the implementation of operational security controls.	5	
		Functional	intersects with	Operations Security Standardized Operating	OPS-01	Mechanisms exist to identify and document Standardized Operating Procedures (SOP),	5	
		Functional	intersects with	Procedures (SOP) Cybersecurity & Data Privacy Portfolio	OPS-01.1 PRM-01	or similar documentation, to enable the proper execution of day-to-day / assigned tasks. Mechanisms exist to facilitate the implementation of cybersecurity & data privacy- related resource planning controls that define a viable plan for achieving cybersecurity	5	
		Functional	intersects with	Management Cybersecurity & Data Privacy Requirements Definition	PRM-05	& data privacy objectives. Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
		Functional	intersects with	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	5	
		Functional	intersects with	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5	
		Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
CC2.2-POF1	Communicates Internal Control Information	Functional	intersects with	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or existenses based on industry-recognized standards to achieve the specific goals of the process area.	5	



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
CC2.2-POF2	Communicates With the Board of Directors	Functional	equal	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	10	
		Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
		Functional	intersects with	Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.	5	
CC2.2-POF3	Provides Separate Communication Lines	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 & data privacy-related incidents.	5	
		Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
		Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies. Mechanisms exist to establish contact with selected groups and associations within the	5	
CC2.2-POF4	Selects Relevant Method of Communication	Functional	intersects with	Contacts With Groups & Associations	GOV-07	cybersecurity & data privacy communities to: - Facilitate ongoing sybersecurity & data privacy education and training for organizational personnel; - Maintain curreny with recommended cybersecurity & data privacy practices, techniques and technologies; and - Share current cybersecurity and/or data privacy-related information including threats, vulnerabilities and incidents.	5	
		Functional	equal	Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.	10	
CC2.2-POF5	Communicates Responsibilities	Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and	5	
		Functional	intersects with	Incident Handling	IRO-02	External Service Providers (ESPs). Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
		Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
CC2.2-POF6	Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters	Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	5	
		Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: Internal stakeholders; Affected clients & third-parties; and Regulatory authorities.	5	
		Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
		Functional	intersects with	Coordination With External Providers Publishing Cybersecurity &	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers. Mechanisms exist to establish, maintain and disseminate cybersecurity & data	5	
		Functional	intersects with	Data Protection Documentation	GOV-02	protection policies, standards and procedures.	5	
CC2.2-POF7	Communicates Objectives and Changes to Objectives	Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
		Functional	intersects with	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5	
		Functional	intersects with	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
CC2.2-POF8	Communicates Information to Improve Security Knowledge and Awareness	Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
		Functional	intersects with	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity & data privacy awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
		Functional	intersects with	Sensitive Information Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive information is formally trained in data handling requirements.	5	
		Functional	intersects with	Privileged Users	SAT-03.5	Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities	5	
CC2.2-POF9	Communicates Information to Improve Privacy Knowledge and Awareness	Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
		Functional	intersects with	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity & data privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	
		Functional	intersects with	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
		Functional	intersects with	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the mission of the organization. Mechanisms exist to implement and govern processes and documentation to facilitate	5	
CC2.2-POF10	Communicates Incident Reporting Methods	Functional	intersects with	Incident Response Operations	IRO-01	an organization-wide response capability for cybersecurity & data privacy-related incidents. Mechanisms exist to cover the preparation, automated detection or intake of incident	5	
		Functional	intersects with	Incident Handling Incident Classification & Prioritization	IRO-02 IRO-02.4	reporting, analysis, containment, eradication and recovery. Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5	
		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.	5	
		Functional	intersects with	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties).	5	
		Functional	intersects with	Control Applicability Boundary Graphical Representation	AST-04.2	Mechanisms exist to ensure control applicability is appropriately-determined for systems, applications, services and third parties by graphically representing applicable boundaries.	5	
CC2.2-POF11	Communicates Information About System Operation and Boundaries	Functional	intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
		Functional	intersects with	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the data and systems under review.	5	
		Functional	intersects with	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	5	
		Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
CC2.2-POF12	Communicates System Objectives	Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
		Functional	intersects with	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: - Before authorizing access to the system or performing assigned duties; - When required by system changes; and - Annually thereafter.	5	
		Functional	intersects with	Change Management Program Configuration Change	CHG-01	Mechanisms exist to facilitate the implementation of a change management program. Mechanisms exist to govern the technical configuration change control processes.	5	
1		Functional	intersects with	Control	CHG-02		5	



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF N	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
		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	
CC2.2-POF13	Communicates System Changes	Functional	intersects with	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: - Before authorizing access to the system or performing assigned duties; - When required by system changes; and - Annually thereafter.	5	
		Functional	intersects with	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
		Functional	intersects with	Statutory, Regulatory & Contractual Compliance Cybersecurity & Data	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. Mechanisms exist to provide a cybersecurity & data protection controls oversight	5	
		Functional	intersects with	Protection Controls Oversight	CPL-02	function that reports to the organization's executive leadership.	5	
		Functional	intersects with	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies. Mechanisms exist to establish contact with selected groups and associations within the	5	
CC2.3	COSO Principle 15	Functional	intersects with	Contacts With Groups & Associations	GOV-07	cybensecutify & data privacy communities to: **realitate enging (sybenecutify & data privacy education and training for organizational personnel; **Maintain current with recommended cybensecutify & data privacy practices, techniques and technologies; and **Share current cybensecutify and/or data privacy-related information including threats, vulnerabilities and incidents.	5	
		Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: Internal stakeholders; Affected clients & third-parties; and Regulatory authorities.	5	
		Functional	intersects with	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies. Mechanisms exist to maintain data privacy-related records and develop, disseminate	5	
		Functional	intersects with	Data Privacy Records & Reporting	PRI-14	and update reports to internal senior management, as well as external oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory data privacy program mandates. Mechanisms exist to timely-report incidents to applicable:	5	
		Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Internal stakeholders; Affected clients & third-parties; and Regulatory authorities.	5	
CC2.3-POF1	Communicates to External Parties	Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
		Functional	intersects with	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity & data privacy incident information to the provider of the product or service and other organizations involved in the supply chain for systems or system components related to the incident.	5	
		Functional	intersects with	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	5	
CC2.3-POF2	Enables inbound Communications	Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
		Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
CC2.3-POF3	Communicates With the Board of Directors	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
CC2.5+OF3		Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
CC2.3-POF4	Provides Separate Communication Lines	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
		Functional	intersects with	Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.	5	
		Functional	intersects with	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
CC2.3-POF5	Selects Relevant Method of Communication	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
		Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. Mechanisms exist to define supporting business processes and implement appropriate	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
CC2.3-POF6	Communicates Objectives Related to Confidentiality and Changes to Those Objectives	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
		Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for Cyberscutrity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
		Functional	intersects with	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data privacy controls.	5	
CC2.3-POF7	Communicates Objectives Related to Privacy and Changes to Those Objectives	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: Abide data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; I share the state of t	5	
		Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
		Functional	intersects with	Incident Handling Incident Response Plan	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery. Mechanisms exist to maintain and make available a current and viable incident	5	
CC2.3-POF8	Communicates Incident Reporting Methods	Functional	intersects with	(IRP) Situational Awareness For	IRO-04	Response Plan (IRP) to all stakeholders. Mechanisms exist to document, monitor and report the status of cybersecurity & data	5	
CC2.5-PUF8	communicaces munera reporting methods	Functional	intersects with	Incidents	IRO-09	privacy incidents to internal stakeholders all the way through the resolution of the incident. Mechanisms exist to timely-report incidents to applicable:	5	
		Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Internal stakeholders; Affected clients & third-parties; and Regulatory authorities. Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar	5	
		Functional	subset of	System Security & Privacy Plan (SSPP)	IAO-03	document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	10	
CC2.3-POF9	nmunicates Information About System Operation and Boundaries	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
		Functional	subset of	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecutity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	10	



FDE#	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
				System Security & Privacy		Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each	(optional)	
		Functional	intersects with	Plan (SSPP)	IAO-03	critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	5	
CC2.3-POF10	Communicates System Objectives	Functional	intersects with	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
		Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
		Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
		Functional	intersects with	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on ach chitical system, application or service, as well as influence inputs, entitles, systems, applications and processes, providing a historical record of the data and its origins.	5	
CC2.3-POF11	Communicates System Responsibilities	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
		Functional	subset of	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	systems, processes and usua. Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and	10	
		Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	External Service Providers (ESPs). Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
		Functional	intersects with	Coordination With External	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	5	
				Providers Suspicious		Mechanisms exist to provide training to personnel on organization-defined indicators of		
		Functional	intersects with	Communications & Anomalous System Behavior	SAT-03.2	malware to recognize suspicious communications and anomalous behavior. Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC2.3-POF12	Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters	Functional	intersects with	Third-Party Management	TPM-01	mechanisms exist to racilitate the implementation of uniro-party management controls.	5	
		Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
		Functional	intersects with	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected systems, applications and/or services that the organization utilizes.	5	
		Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
		Functional	subset of	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	10	
		Functional	intersects with	Cybersecurity & Data Privacy Portfolio	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy- related resource planning controls that define a viable plan for achieving cybersecurity	5	
		Functional	intersects with	Management Cybersecurity & Data Privacy In Project	PRM-04	& data privacy objectives. Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly,	5	
		· uncoolidi	microecio With	Management	. Aw-04	operating as intended and producing the desired outcome with respect to meeting the requirements. Mechanisms exist to define business processes with consideration for cybersecurity &	,	
CC3.1	COSO Principle 6	Functional	intersects with	Business Process Definition	PRM-06	data privacy that determines: • The resulting risk to organizational operations, assets, individuals and other organizations; and	5	
						 Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained. 		
		Functional	intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
		Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		Functional	intersects with	Alignment With Enterprise Architecture	SEA-02	and information grant manage against unose plants. Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other	5	
		Functional	intersects with	Define Control Objectives	GOV-09	organizations. Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5	
		Functional	intersects with	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the mission of the organization.	5	
						Mechanisms exist to identify: - Assumptions affecting risk assessments, risk response and risk monitoring; - Constraints affecting risk assessments. risk response and risk monitoring:		
CC3.1-POF1	Reflects Management's Choices	Functional	intersects with	Risk Framing	RSK-01.1	The organizational risk tolerance; and Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
		Functional	intersects with	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
		Functional	intersects with	Risk Threshold	RSK-01.4	Mechanisms exist to define organizational risk threshold, the level of risk exposure above which risks are addressed and below which risks may be accepted.	5	
		Functional	intersects with	Risk Appetite		Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	5	
		Functional	equal	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	10	
CC3.1-POF2	Considers Tolerances for Risk	Functional	intersects with	Risk Threshold	RSK-01.4	Mechanisms exist to define organizational risk threshold, the level of risk exposure above which risks are addressed and below which risks may be accepted.	5	
		Functional	intersects with	Risk Appetite Defining Business Context	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward. Mechanisms exist to define the context of its business model and document the	5	
		Functional	intersects with	Befining Business Context & Mission	GOV-08	mission of the organization. Mechanisms exist to identify:	5	
CC3.1-POF3	Includes Operations and Financial Performance Goals	Functional	intersects with	Risk Framing	RSK-01.1	 Assumptions affecting risk assessments, risk response and risk monitoring; Constraints affecting risk assessments, risk response and risk monitoring; The organizational risk tolerance, and Priorities, benefits and trade-offs considered by the organization for managing risk. 	5	
		Functional	intersects with	Cybersecurity & Data Privacy Portfolio Management		Mechanisms exist to facilitate the implementation of cybersecurity & data privacy- related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	5	
CC3.1-POF4	Forms a Basis for Committing of Resources	Functional	intersects with	Allocation of Resources		as data privacy objectives. Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.	5	
CC2 1 DC	Familier With Applicable Accounting Standards	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	initiatives. Machanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
CC3.1-POF5	Complies With Applicable Accounting Standards	Functional	intersects with	Statutory, Regulatory & Contractual Compliance		Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
		Functional	intersects with	Materiality Determination	GOV-16	Mechanisms exist to define materiality threshold criteria capable of designating an incident as material to the organization.	5	
CC3.1-POF6	Considers Materiality	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: - Assumptions affecting risk assessments, risk response and risk monitoring: - Constraints affecting risk assessments, risk response and risk monitoring: - The organizational risk tolerance; and - Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
		Functional	intersects with	Risk Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security yulnerabilities that is based on industry-recognized practices.	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
CC3.1-POF7	effects Entity Activities	Functional	intersects with	Business Process Definition		Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: *The resulting risk to organizations and organizations assets, individuals and other organizations.	5	
						 Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained. 		



Part	FDE II Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF II	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
### 1845		Functional	intersects with	Define Control Objectives	GOV-09		(optional) 5	
Part		Functional	intersects with		CPL-01		5	
Part	CC3.1-POF8 Compiles With Externally Established Frameworks	Functional	intersects with	Service Delivery	OPS-03	Mechanism exist to define supporting business processes and implement appropriate governance and service management or neurue appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, worldroze, and/or sustomers based on industry-recognized standards to achieve the specific goals of the process area.	5	
Handle Market		Functional	intersects with	Business Process Definition	PRM-06	data privacy that determines: • The resulting risk to organizational operations, assets, individuals and other organizations; and • Information protection needs arising from the defined business processes and revises	5	
1		Functional	intersects with	Define Control Objectives	GOV-09		5	
1		Functional	intersects with		CPL-01		5	
# 1	CC3.1-POF9 Considers the Required Level of Precision	Functional	intersects with	Service Delivery	OPS-03	governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
지 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		Functional	intersects with	Business Process Definition	PRM-06	data privacy that determines: • The resulting risk to organizational operations, assets, individuals and other organizations; and • Information protection needs arising from the defined business processes and revises	5	
1				Governing Body		those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.		
						enforcement and regulatory bodies. Mechanisms exist to submit status reporting of the organization's cybersecurity and/or		
	CC3.1-POF10 Reflects Entity Activities			Privacy Status Reporting Service Delivery		data privacy program to applicable statutory and/or regulatory authorities, as required. Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the		
Part		Functional	intersects with	Business Process Definition	PRM-06	data privacy that determines: • The resulting risk to organizational operations, assets, individuals and other organizations; and • Information protection needs arising from the defined business processes and revises	5	
Registration Regi		Functional	intersects with		GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
Ministration Mini		Functional	intersects with		GOV-01.2	those entrusted to make executive decisions about matters considered material to the	5	
Part	CC3.1-POF11 Reflects Management's Choices	Functional	intersects with		OPS-03	governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the	5	
Publicated and Procession of P		Functional	intersects with	Business Process Definition	PRM-06	data privacy that determines: • The resulting risk to organizational operations, assets, individuals and other organizations; and • Information protection needs arising from the defined business processes and revises	5	
Functional interacts with seasons process and requirements appropriate and programments and programments appropriate and programments and programments appropriate and programments appropriate and process and requirements appropriate and programments appropriate and process and requirement appropriate appr		Functional	intersects with		OPS-03	governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the	5	
Purticional Interest sub Intere	CC3.1-POF12 Considers the Required Level of Precision	Functional	intersects with	Business Process Definition	PRM-06	data privacy that determines: • The resulting risk to organizational operations, assets, individuals and other organizations; and • Information protection needs arising from the defined business processes and revises	5	
Functional subset of Control Complex with Business Process Definition PPM-06 processes are necessary, well an authorise of the processes are sensors, well an authorise of the processes and implement appropriate promonance and sensor processes and implement appropriate promonance and sensor processes and implement appropriate promonance and sensor processes and implement appropriate promonance and sensor processes with consideration for opheraccurity & processes and implement appropriate promonance and sensor processes with consideration for opheraccurity & processes and incomment appropriate promonance and sensor processes and incomment appropriate promonance and sensors processes and incomment appropriate promonance and sensors processes and incomment appropriate promonance and sensors are processes and incomment appr		Functional	intersects with		OPS-03	governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the	5	
Functional intersects with Punctional Punct	CC3.3-90P13 Reflects Entity Activities	Functional	intersects with	Business Process Definition	PRM-06	data privacy that determines: • The resulting risk to organizational operations, assets, individuals and other organizations; and • Information protection needs arising from the defined business processes and revises	5	
Functional intersects with Service Delivery (Business Process Support) Reflects External Laws and Regulations Functional intersects with Business Process Definition with Control Objectives and Process Support of the organizations technology capabilities supporting business functions, so an intersect swith surface and service management to ensure appropriate planning, delivery and support of the organizations in consumer planning of services and revises the participant of the process area. Functional intersects with Business Process Definition PRIA-00 Functional intersects with Define Control Objectives (Business Process Support) Functional intersects with Define Control Objectives (Business Process Support) Functional intersects with Business Process Definition intersects with Define Control Objectives and management to ensure appropriate planning, delivery and support of the organizations in control objectives and revises the passes for the selection, membrane and the process are necessary, until an archiveable set of protection needs to deline the context of its business model and document the mission of the organizations comparizations control objectives as the basis for the selection, membrane and management of percentage size to ask as privacy that determines: Functional intersects with Define Control Objectives (GO-99) Service Delivery (Business Process Support) Functional intersects with Define Control Objectives (GO-99) Service Delivery (Business Process Support) Functional intersects with Business Process Support (Business Process and implement appropriate governance and evolve the process are necessary, until an archive planning, delivery and support of the organizations in control objectives and evolve the process are an existent to define apparation control objective and individual and other control objective and individual and other process and revises the process and r		Functional	subset of		CPL-01	statutory, regulatory and contractual controls.	10	
Functional intersects with Business Process Definition PRM-66 Functional intersects with Business Process Definition PRM-66 Functional intersects with Prunctional intersects with Business Process Definition PRM-66 Functional intersects with Risk Tolerance RS-Call Sequence Process Sea necessary, until an anchievable set of protection needs arising from the defined business processes and revises the processor as an extensive to define supporting business processes and implement appropriate generated and service management of the organization's internal accord of system. 5 Mechanisms exist to define supporting business processes and implement appropriate generated and service management to ensure appropriate planning, delivery and support of the organization Section Section Sequence Section (PM-66) Functional intersects with Business Process Support of the organization Section Sec	CC3.1-PDF14 Reflects External Laws and Regulations	Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
Functional intersects with Define Control Objectives GOV-99 implementation and management of the organization's internal control objectives as the basis for the selection, internal control objectives and the organization's internal control objectives as the basis for the selection, internal control objection selection internal control objection as the basis for the organization objectives as the basis for the selection, in		Functional	intersects with	Business Process Definition	PRM-06	data privacy that determines: • The resulting risk to organizational operations, assets, individuals and other organizations; and • Information protection needs arising from the defined business processes and revises	5	
Functional intersects with Define Control Objectives GOV-09 implementation and management of the organization's internal control system. Exercise Delivery (Business Process Support) CC3.1-POF15 Considers Tolerances for Risk Functional intersects with Business Process Definition PRM-06 Functional intersects with Risk Tolerance Functional intersects with Risk Tolerance Risk Tolerance Functional intersects with Risk Tolerance Risk Tolerance Risk Intersects to define organizational and anchievable set of protection needs and indicate least on enganizational and anchievable set of protection needs and revises the processes are necessary, until an achievable set of protection needs and anchievable set of protection needs and anchievab		Functional	intersects with	Defining Business Context & Mission	GOV-08	mission of the organization.	5	
CC3.1-PDF15 Considers Tolerances for Risk CC3.1-PDF15 CC3.1-PDF15 Considers Tolerances for Risk CC3.1-PDF15 Considers Tolerance for Risk CC3.1-PDF15 Considers Tolerance for Risk Toleranc		Functional	intersects with	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5	
CC3.1-POF15 Considers Tolerances for Risk Functional intersects with Business Process Definition PPBM-06 Prescribing risk to againstational operations, assets, individuals and other organizational operations, assets, individuals and other organizations, and information protection needs arising from the defined business processes and reviews the processes an energy in an anchevable set of protection needs in obtained. Functional PRISK Tolerance		Functional	intersects with		OPS-03	governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
resiscus with the second secon	CC3.1-POF1S Considers Tolerances for Risk	Functional	intersects with	Business Process Definition	PRM-06	data privacy that determines: The resulting risk to organizational operations, assets, individuals and other organizations; and Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	_
Mechanisms exist to define organizational risk threshold, the level of risk exposure Eurortional intercarts with Bick Threshold BECLET A Boban within the risk and manufactured and the accounted to		Functional	intersects with	Risk Tolerance	RSK-01.3	acceptable results.	5	
Functional intersects with not intersect with not the sum of the s		Functional	intersects with	Risk Threshold	RSK-01.4	Mechanisms exist to define organizational risk threshold, the level of risk exposure above which risks are addressed and below which risks may be accepted.	5	



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
		Functional	intersects with	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	(optional) 5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate poverance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
CC3.1-POF16	Establishes Sub-Objectives for Risk Assessment	Functional	intersects with	Business Process Definition	PRM-06	Mechanism exist to define business processes with consideration for cybersecurity & data provery that determines: - The resulting risk to organizational operation, assets, individuals and other organizations; and in the organizations and in the organizations; and in the organization protection needs arising from the defined business processes and revises the processes are necessary, until an archievable set of protection needs is obtained.	5	
		Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: - Assumptions affecting risk assessments, risk response and risk monitoring: - Constraints affecting risk assessments, risk response and risk monitoring: - The organizational risk tolerance; and - Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
		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 systems and data.	5	
		Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: - Assumptions affecting risk assessments, risk response and risk monitoring; - Constraints affecting risk assessments, risk response and risk monitoring; - Constraints affecting risk assessments, risk response and risk monitoring; - Constraints affecting risk assessments and risk promotion and risk or organization for managing risk.	5	
		Functional	equal	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	10	
<i></i>	onsiders Tolerances for Risk	Functional	intersects with	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize systems and data in accordance with applicable local, state and federal laws that: - Document the security categorization results (including supporting rationale) in the security plan for systems; and - Ensure the security categorization decision is reviewed and approved by the asset owner.	5	
CC3.2	Considers Tolerances for Risk	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
		Functional	intersects with	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks. Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM)	5	
		Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans. Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems,	5	
		Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
		Functional	intersects with	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services. Mechanisms exist to facilitate the implementation of strategic, operational and tactical	5	
		Functional	subset of	Risk Management Program	RSK-01	risk management controls.	10	
CC3.2-POF1	Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
		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 systems and data.	5	
		Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: - Assumptions affecting risk assessments, risk response and risk monitoring: - Constraints affecting risk assessments, risk response and risk monitoring: - Constraints affecting risk assessments, risk response and risk monitoring: - The organizational risk tolerance, and - Prioritties, benefits and trade-offs considered by the organization for managing risk.	5	
CC3.2-POF2	Analyzes Internal and External Factors	Functional	subset of	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	10	
		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 systems and data.	5	
		Functional	intersects with	Cybersecurity & Data Privacy Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	5	
CC3.2-POF3	Involves Appropriate Levels of Management	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
		Functional	equal	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 systems and data.	10	
CC3.2-POF4	Estimates Significance of Risks Identified	Functional	intersects with	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for systems, applications and/or services to prevent potential disruptions. Mechanisms exist to identify and assign a risk ranking to newly discovered security	5	
		Functional	intersects with	Risk Ranking Risk Management Program	RSK-05 RSK-01	vulnerabilities that is based on industry-recognized practices. Mechanisms exist to facilitate the implementation of strategic, operational and tactical	5	
CC3.2-POF5	Determines How to Respond to Risks	Functional	equal	Risk Response		risk management controls. Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	10	
		Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external. Mechanisms exist to develop and keep current a catalog of applicable risks associated	5	
		Functional	intersects with	Risk Catalog	RSK-03.1	with the organization's business operations and technologies in use. Mechanisms exist to conduct recurring assessments of risk that includes the likelihood	5	
		Functional	intersects with	Risk Assessment	RSK-04	mechanisms exist to cinduct recurring assessments or risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data. Mechanisms exist to implement a threat intelligence program that includes a cross-	5	
CC3.2-POF6	Identifies Threats - The entity identifies threats to the achievement of its objectives from intentional (including malicious) and unintentional acts and environmental events.	Functional	subset of	Threat Intelligence Program Indicators of Exposure	THR-01	rectainsistic sexis to implement a united intelligence program than includes a cluss- 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. Mechanisms exist to develop indicators of Exposure (IOE) to understand the potential	10	
		Functional	intersects with	(IOE) Threat Intelligence Feeds	THR-02 THR-03	attack vectors that attackers could use to attack the organization. Mechanisms exist to maintain situational awareness of evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the	5	
		Functional	intersects with	Threat Catalog	THR-09	implementation of preventative and compensating controls. Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
		Functional	intersects with	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5	
		Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management [SCRM] associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		Functional	intersects with	Supply Chain Risk Assessment Threat Intelligence	RSK-09.1 THR-01	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services. Mechanisms exist to implement a threat intelligence program that includes a cross- organization information-sharing capability that can influence the development of the	5	
		Functional	intersects with	Program Indicators of Exposure	THR-02	system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities. Mechanisms exist to develop Indicators of Exposure (IOE) to understand the potential	5	
CC3.2-POF7	Identifies Vulnerability of System Components	Functional	intersects with	(IOE) Threat Intelligence Feeds		attack vectors that attackers could use to attack the organization. Mechanisms exist to maintain situational awareness of evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
		Functional	intersects with	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
	r	Functional	intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
		Functional	intersects with	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities. Mechanisms exist to detect vulnerabilities and configuration errors by routine	5	
		Functional	intersects with	Vulnerability Scanning	VPM-06	wetnessins exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	



FDE#	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF II	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		Rationale	Relationship			Mechanisms exist to identify:	(optional)	
		Functional	intersects with	Risk Framing	RSK-01.1	 Assumptions affecting risk assessments, risk response and risk monitoring; Constraints affecting risk assessments, risk response and risk monitoring; The organizational risk tolerance; and Priorities, benefits and trade-offs considered by the organization for managing risk. 	5	
		Functional	intersects with	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
		Functional	intersects with	Risk Threshold	RSK-01.4	Mechanisms exist to define organizational risk threshold, the level of risk exposure above which risks are addressed and below which risks may be accepted.	5	
		Functional	intersects with	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	5	
CC3.2-POF8	Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties	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 systems and data.	5	
		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	
		Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans. Mechanisms exist to identify, profitze and assess suppliers and partners of critical	5	
		Functional	intersects with	Third-Party Criticality Assessments	TPM-02	systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services. Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing	5	
		Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	of technology-related services. Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External	5	
		Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity & data privacy controls, including any flow-down requirements to subcontractors.	5	
						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 systems and data.		
		Functional	intersects with	Risk Assessment	RSK-04		5	
						Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.		
		Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1		5	
						Mechanisms exist to identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.		
		Functional	intersects with	Third-Party Criticality Assessments	TPM-02		5	
						Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing		
		Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	of technology-related services.	5	
CC3.2-POF9	Assesses the Significance of the Risks					Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.		
		Functional	intersects with	Threat Analysis	THR-10	anu incennuou(s) ur appincaure incernai anu excernai cineass.	5	
		Functional	intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
						Mechanisms exist to define and manage the scope for its attack surface management activities.		
		Functional	intersects with	Attack Surface Scope	VPM-01.1		5	
						Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known		
		Functional	intersects with	Vulnerability Exploitation Analysis	VPM-03.1	vulnerabilities.	5	
		Functional	subset of	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.	10	
		Functional	intersects with	Indicators of Exposure (IOE)	THR-02	Mechanisms exist to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.	5	
CC3.3	COSO Principle 8	Functional	intersects with	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross- discipline insider threat incident handling team. Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC.3.3		Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to utilize tailored acquisition strategies, contract tools and	5	
		Functional	intersects with	Acquisition Strategies, Tools & Methods	TPM-03.1	procurement methods for the purchase of unique systems, system components or services.	5	
		Functional	intersects with	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data. Mechanisms exist to ensure that the interests of external service providers are	5	
 		Functional	intersects with	Conflict of Interests Asset Governance	TPM-04.3 AST-01	consistent with and reflect organizational interests. Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement	5	
		Functional	intersects with	Human Resources Security		and manage asset management controls. Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC3.3-POF1	Considers Various Types of Fraud	Functional	subset of	Management 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.	10	
		Functional	intersects with	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross- discipline insider threat incident handling team.	5	
		Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC3.3-POF2	Assesses Incentives and Pressures	Functional	subset of	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	10	
		Functional	subset of	Insider Threat Program	THR-04	hunting, response and recovery activities. Mechanisms exist to implement an insider threat program that includes a cross-	10	
		runctional	subset or	sider Tilleat Program	111K-04	discipline insider threat incident handling team.	10	l .



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF II	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	(optional) 5	
CC3.3-POF3	Assesses Opportunities	Functional	subset of	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.	10	
		Functional	subset of	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross- discipline insider threat incident handling team.	10	
		Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC3.3-POF4	Assesses Attitudes and Rationalizations	Functional	subset of	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.	10	
		Functional	subset of	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross- discipline insider threat incident handling team.	10	
		Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC3.3-POF5	Considers the Risks Related to the Use of IT and Access to Information	Functional	subset of	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.	10	
		Functional	subset of	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross- discipline insider threat incident handling team.	10	
		Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
		Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes. Mechanisms exist to appropriately test and document proposed changes in a non-	5	
		Functional	intersects with	Test, Validate & Document Changes Cybersecurity & Data	CHG-02.2	production environment before changes are implemented in a production environment. Mechanisms exist to include a cybersecurity and/or data privacy representative in the	5	
		Functional	intersects with	Privacy Representative for Asset Lifecycle Changes	CHG-02.3	configuration change control review process.	5	
		Functional	intersects with	Security Impact Analysis for Changes Cybersecurity & Data	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change. Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-	5	
CC3.4	COSO Principle 9	Functional	intersects with	Privacy Portfolio Management	PRM-01	related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives. Mechanisms exist to define business processes with consideration for cybersecurity &	5	
		Functional	intersects with	Business Process Definition	PRM-06	data privacy that determines: * The resulting risk to organizational operations, assets, individuals and other organizations; and	5	
		Turctoria	mersees wer	business Process Deminion	1 1111 00	Information protection needs arising from the defined business processes and revises the processes a necessary, until an achievable set of protection needs is obtained.	,	
				Third-Party Risk		Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing	_	
		Functional	intersects with	Assessments & Approvals	TPM-04.1	of technology-related services. Mechanisms exist to monitor, regularly review and audit External Service Providers	5	
		Functional	intersects with	Review of Third-Party Services	TPM-08	(ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
		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 information, systems and processes that are in scope by the third-	5	
		Functional	intersects with	Risk Management Program	RSK-01	party. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
CC3.4-POF1	Assesses Changes in the External Environment	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
		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 systems and data.	5	
		Functional	intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
CC3.4-POF2	Assesses Changes in the Business Model	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
		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 systems and data.	5	
		Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
CC3.4-POF3	Assesses Changes in Leadership	Functional	intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
		Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external. Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption,	5	
		Functional	intersects with	Risk Assessment	RSK-04	modification or destruction of the organization's systems and data.	5	
		Functional	intersects with	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
		Functional	intersects with	Configuration Change Control Security Impact Analysis	CHG-02	Mechanisms exist to govern the technical configuration change control processes. Mechanisms exist to analyze proposed changes for potential security impacts, prior to	5	
CC3.4-POF4	Assesses Changes in Systems and Technology	Functional	intersects with	for Changes Risk Management Program	CHG-03 RSK-01	the implementation of the change. Mechanisms exist to facilitate the implementation of strategic, operational and tactical	5	
	<u> </u>	Functional	intersects with	Risk Identification	RSK-03	risk management controls. Mechanisms exist to identify and document risks, both internal and external.	5	
		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 systems and data.	5	
		Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to identify and document risks, both internal and external.	10	
		Functional	intersects with	Risk Identification	RSK-03 RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption,	5	
						modification or destruction of the organization's systems and data. Mechanisms exist to facilitate the implementation of third-party management controls.		
CC3.4-POF5	Assesses Changes in Vendor and Business Partner Relationships	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to perform recurring validation of the Responsible, Accountable,	10	
		Functional	intersects with	Third-Party Scope Review	TPM-05.5	Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity & data privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	
		Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
		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 information, systems and processes that are in scope by the third- party. Machanisms exist to implement a threat intelligence program that includes a cross.	5	
		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.	5	
		Functional	intersects with	Threat Analysis Vulnerability & Patch	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats. Mechanisms exist to facilitate the implementation and monitoring of vulnerability	5	
		Functional	intersects with	Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
CC3.4-POF6	Assesses Changes in Threats and Vulnerabilities	Functional	intersects with	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
		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. Mechanisms exist to identify, assess, prioritize and document the potential impact(s)	5	
		Functional	intersects with	Vulnerability Exploitation Analysis	VPM-03.1	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.	5	
		•						•



FDE#	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	(optional) 5	
		Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	5	
		Functional	intersects with	Functional Review Of Cybersecurity & Data	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	
		Functional	intersects with	Protection Controls 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	5	
	-	Functional	intersects with	Measures of Performance	GOV-05	operations. Mechanisms exist to develop, report and monitor cybersecurity & data privacy program	5	
		Functional	intersects with	Key Performance Indicators (KPIs)	GOV-05.1	measures of performance. Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring and trend analysis of the	5	
		Functional	intersects with	Key Risk Indicators (KRIs)	GOV-05.2	cybersecurity & data privacy program. Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the cybersecurity	5	
		Functional	intersects with	Information Assurance (IA)	IAO-01	& data privacy program. Mechanisms exist to facilitate the implementation of cybersecurity & data privacy	5	
		Functional	intersects with	Operations Assessments	IAO-02	assessment and authorization controls. Mechanisme seix to formally assess the cybersecurity & data privacy controls in systems, applications and services through information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting	5	
		Functional	intersects with	Assessor Independence	IAO-02.1	expected requirements. Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct cybersecurity & data privacy control assessments.	5	
CC4.1	COSO Principle 16	Functional	intersects with	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: **Statutor, regulatory and contractual compliance obligations; **Monitoring capabilities; **Notile devices; **Publication scartify, **Application scartify, **Application scartify, **Vulnerability management; **Vulnerability management; **Indiaction score; **Indiactive score; *	5	
		Functional	intersects with	Plan / Coordinate with Other Organizational	IAO-03.1	Mechanisms exist to plan and coordinate Information Assurance Program (IAP) activities with affected stakeholders before conducting such activities in order to reduce the potential impact on operations.	5	
		Functional	intersects with	Entities Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Test and Evaluation (ST&E) plan to identify and remediate flaws during development.	5	
		Functional	intersects with	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical cybersecurity & data privacy controls.	5	
		Functional	intersects with	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects /	5	
		Functional	intersects with	Cybersecurity & Data Privacy In Project Management	PRM-04	initiatives. Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the	5	
		Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	requirements. Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
		Functional	intersects with	Business Process Definition	PRM-06	Mechanism exist to define business processes with consideration for cybensecurity & data princip that determines: "The resulting risk to organizational operations, assets, individuals and other organizations, and "Information protection needs arising from the defined business processes and revises the processes as necessary, until an adviseable set of protection needs is obtained."	5	
		Functional	intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
		Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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 cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
		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.	5	
CC4.1-POF1	Considers a Mix of Ongoing and Separate Evaluations	Functional	intersects with	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy personnel to: - Create and implement a Security Test and Evaluation (\$T&E) plan; implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and - Document the results of the security testing/evaluation and flaw remediation processes.	5	
		Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
CC4.1-POF2	Considers Rate of Change	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.	5	
CC4.1-POF3	Establishes Baseline Understanding	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.	5	
		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.	5	
CC4.1-POF4	Uses Knowledgeable Personnel	Functional	intersects with	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: - Statutory, regulatory and contractual compliance obligations; - Monitoring capabilities; - Motible devices; - Databases;	5	
CC4.1-POF5	Integrates With Business Processes	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.	5	
CC4.1-POF6	Adjusts Scope and Frequency	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.	5	
CC4.1-POF7	Objectively Evaluates	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.	5	
		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.	5	
CC4.1-POF8	Considers Different Types of Ongoing and Separate Evaluations	Functional	intersects with	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	5	
		Functional	intersects with	Assessments	IAO-02	Mechanism exist to formally assess the cybersecurity & data privacy controls in systems, applications and services through information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as informed and producing the desired outcome with respect to meeting expected requirements.	5	



FDE#	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		Functional	intersects with	Steering Committee &	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data	(optional)	
		Functional	intersects with	Program Oversight Status Reporting To	GOV-01.2	privacy and business executives, which meets formally and on a regular basis. Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the	5	
				Governing Body		organization's cybersecurity & data protection program. Mechanisms exist to document and review instances of non-compliance with statutory,		
		Functional	intersects with	Non-Compliance Oversight Threat Analysis & Flaw	CPL-01.1	regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to require system developers and integrators to create and execute a	5	
		Functional	intersects with	Remediation During Development	IAO-04	Security Test and Evaluation (ST&E) plan to identify and remediate flaws during development. Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk	5	
CC4.2	COSO Principle 17	Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known yulnerabilities.	5	
		Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
		Functional	intersects with	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.	5	
		Functional	intersects with	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
		Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
		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.	5	
		Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Status Reporting To	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the	5	
		Functional	intersects with	Governing Body Measures of Performance	GOV-05	organization's cybersecurity & data protection program. Mechanisms exist to develop, report and monitor cybersecurity & data privacy program	5	
CC4.2-POF1	Assesses Results	Functional	intersects with	Non-Compliance Oversight	CPL-01.1	measures of performance. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
		Functional	intersects with	Cybersecurity & Data Protection Controls	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
		Functional	intersects with	Oversight Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required cybersecurity & data privacy controls for each system, application and/or service under	5	
				Steering Committee &		their control are implemented correctly and are operating as intended. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data		
		Functional	intersects with	Program Oversight	GOV-01.1	privacy and business executives, which meets formally and on a regular basis. Mechanisms exist to provide governance oversight reporting and recommendations to	5	
CC4.2-POF2	Communicates Deficiencies	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
		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	
		Functional	intersects with	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
		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	
CC4.2-POF3	Monitors Corrective Action	Functional	intersects with	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
		Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
		Functional	intersects with	Risk Register Operationalizing	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks. Mechanisms exist to compel data and/or process owners to operationalize	5	
		Functional	intersects with	Cybersecurity & Data Protection Practices	GOV-15	cybersecurity & data privacy practices for each system, application and/or service under their control. Mechanisms exist to compel data and/or process owners to select required	5	
		Functional	intersects with	Select Controls	GOV-15.1	rectains sexist to competitions and/or process owners to serect required cybersecurity & data privacy controls for each system, application and/or service under their control. Mechanisms exist to compel data and/or process owners to implement required	5	
		Functional	intersects with	Implement Controls	GOV-15.2	cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
		Functional	intersects with	Separation of Duties (SoD) Standardized Operating	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion. Mechanisms exist to identify and document Standardized Operating Procedures (SOP),	5	
		Functional	intersects with	Procedures (SOP)	OPS-01.1	or similar documentation, to enable the proper execution of day-to-day / assigned tasks. Mechanisms exist to develop a security Concept of Operations (CONOPS), or a similarly-	5	
		Functional	intersects with	Security Concept Of Operations (CONOPS)	OPS-02	defined plan for achieving cybersecurity objectives, that documents management, operational and technical measures implemented to apply defense-in-depth techniques that is communicated to all appropriate stakeholders.	5	
CC5.1	COSO Principle 10					Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines:		
		Functional	intersects with	Business Process Definition	PRM-06	 Information protection needs arising from the defined business processes and revises 	5	
		Functional	intersects with	Risk Management Program	RSK-01	the processes as necessary, until an achievable set of protection needs is obtained. Mechanisms exist to facilitate the implementation of strategic, operational and tactical	5	
		Functional	intersects with	Secure Engineering	SEA-01	risk management controls. Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and	5	
		Functional	intersects with	Principles Centralized Management of Cybersecurity & Data	SEA-01.1	modification of systems and services. Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity & data privacy controls and related processes.	5	
		Functional	intersects with	Privacy Controls Alignment With Enterprise	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry- recognized leading practices, with consideration for cybersecurity & data privacy	5	
CC5.1-POF1	Integrates With Risk Assessment	Functional	intersects with	Architecture Operationalizing Cybersecurity & Data	GOV-15	principles that addresses risk to organizational operations, assets, individuals, other organizations. Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under	5	
-		Functional	intersects with	Protection Practices Defining Business Context	GOV-08	their control. Mechanisms exist to define the context of its business model and document the mission of the organization.	5	
CC5.1-POF2	Considers Entity-Specific Factors	Functional	intersects with	& Mission Operationalizing Cybersecurity & Data	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under	5	
CC5.1-POF3	Determines Relevant Business Processes	Functional	intersects with	Protection Practices Operationalizing	GOV-15	their control. Mechanisms exist to compel data and/or process owners to operationalize	5	
CC5.1-POF4	Determines Relevant Business Processes Evaluates a Mix of Control Activity Types	Functional	intersects with	Cybersecurity & Data Protection Practices Operationalizing Cybersecurity & Data	GOV-15	cybersecurity & data privacy practices for each system, application and/or service under their control. Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under	5	
		Functional	intersects with	Protection Practices Operationalizing Cybersecurity & Data	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under	5	
CC5.1-POF5	Considers at What Level Activities Are Applied	Functional	intersects with	Protection Practices Targeted Capability	PRM-01.2	Eyer security a use privacy produces for each system, approached anyon service under their control. Mechanisms exist to define and identify targeted capability maturity levels.	5	
CCE 1 POPP	Addresses Correction of Pulice	Functional	intersects with	Maturity Levels Operationalizing Cybersecurity & Data	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under	5	
CC5.1-POF6	Addresses Segregation of Duties	Functional	intersects with	Protection Practices Separation of Duties (SoD)	HRS-11	their control. Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
	· · · · · · · · · · · · · · · · · · ·			-		· · · · · · · · · · · · · · · · · · ·		



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF II	Secure Controls Framework (SCF) Control Description	Strength of Relationship (ontional)	Notes (optional)
		Functional	intersects with	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy- related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	5	
		Functional	intersects with	Cybersecurity & Data Privacy In Project	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the	5	
		Functional	intersects with	Management Cybersecurity & Data Privacy Requirements	PRM-05	requirements. Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined	5	
		runctional	intersects with	Definition	PRIVI-03	decision points in the Secure Development Life Cycle (SDLC). Mechanisms exist to define business processes with consideration for cybersecurity &	,	
		Functional	intersects with	Business Process Definition	PRM-06	data privacy that determines: • The resulting risk to organizational operations, assets, individuals and other organizations; and	5	
CC5.2	COSO Principle 11					 Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained. 		
		Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
		Functional	intersects with	Business Impact Analysis (BIA) Data Protection Impact	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks. Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems,	5	
		Functional		Assessment (DPIA) Secure Engineering	RSK-10	applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks. Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity	5	
		Functional	intersects with	Principles Technology Development	SEA-01 TDA-01	& data privacy practices in the specification, design, development, implementation and modification of systems and services. Mechanisms exist to facilitate the implementation of tailored development and	5	
		Functional	intersects with	& Acquisition Minimum Viable Product (MVP) Security	TDA-02	acquisition strategies, contract tools and procurement methods to meet unique business needs. Mechanisms exist to ensure risk-based technical and functional specifications are established to define a Minimum Viable Product (MVP).	5	
CC5.2-POF1	Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls	Functional	equal	Requirements Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of technology assets that support more than one critical business function.	10	
		Functional	intersects with	Control Applicability Boundary Graphical Representation	AST-04.2	Mechanisms exist to ensure control applicability is appropriately-determined for systems, applications, services and third parties by graphically representing applicable	5	
CC5.2-POF2	Establishes Relevant Technology Infrastructure Control Activities	Functional	intersects with	Compliance Scope	CPL-01.2	boundaries. Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
		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	
CC5.2-POF3	Establishes Relevant Security Management Process Controls Activities	Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
		Functional	intersects with	Least Privilege	IAC-21	Mechanism sosts 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	
CC5.2-POF4	Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities	Functional	equal	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.	10	
		Functional	intersects with	Publishing Cybersecurity & Data Protection	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
		Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
CC5.3	COSO Principle 12	Functional	intersects with	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
		Functional	intersects with	Third-Party Personnel Security	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third- party cybersecurity & data privacy roles and responsibilities.	5	
		Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
CC5.3-POF1	Establishes Policies and Procedures to Support Deployment of Management's Directives	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures. Mechanisms exist to incorporate cybersecurity & data privacy principles into Business	5	
		Functional	intersects with	Business As Usual (BAU) Secure Practices Assigned Cybersecurity &	GOV-14	As Usual (BAU) practices through executive leadership involvement. Mechanisms exist to assign one or more qualified individuals with the mission and	5	
		Functional	intersects with	Data Protection Responsibilities	GOV-04	resources to controlly-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program. Mechanisms exist to enforce an accountability structure so that appropriate teams and	5	
CC5.3-POF2	Establishes Responsibility and Accountability for Executing Policies and Procedures	Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1	individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks. Mechanisms exist to define cybersecurity responsibilities for all personnel.	5	
		Functional	intersects with	Roles & Responsibilities	HRS-03	Mechanisms exist to identify and document Standardized Operating Procedures (SOP).	5	
		Functional	intersects with	Standardized Operating Procedures (SOP)		or similar documentation, to enable the proper execution of day-to-day / assigned tasks. Mechanisms exist to define supporting business processes and implement appropriate	5	
CC5.3-POF3	Performs in a Timely Manner	Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
CC5.3-POF4	Takes Corrective Action	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
		Functional	intersects with	Vulnerability Remediation Process Al & Autonomous	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated. Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies [AAT_related operator and practitioner proficiency requirements for Artificial	5	
CC5.3-POF5	Performs Using Competent Personnel	Functional	intersects with	Technologies Stakeholder Competencies	AAT-13.1	(AAT)-related operator and practitioner proficiency requirements for Artificial intelligence (AI) and Autonomous Technologies (AAT) are defined, assessed and documented. Mechanisms exist to ensure that all security-related positions are staffed by qualified	5	
		Functional	intersects with	Competency Requirements for Security-Related Positions	HRS-03.2	wechanisms exist to ensure that an security-related positions are statted by qualified individuals who have the necessary skill set.	5	
CC5.3-POF6	Reassesses Policies and Procedures	Functional	equal	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	10	
		Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance. Mechanisms exist to facilitate the implementation of cryptographic protections controls	5	
		Functional	intersects with	Use of Cryptographic Controls Transmission	CRY-01 CRY-03	using known public standards and trusted cryptographic technologies. Cryptographic mechanisms exist to protect the confidentiality of data being	5	
		Functional	intersects with	Confidentiality Encrypting Data At Rest	CRY-03 CRY-05	transmitted. Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
		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	
		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. Mechanisms exist to facilitate the production and management of symmetric	5	
		Functional	intersects with	Symmetric Keys	CRY-09.1	cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes. Mechanisms exist to facilitate the production and management of asymmetric	5	
		Functional	intersects with	Asymmetric Keys	CRY-09.2	cryptographic keys using Federal information Processing Standards (FIPS)-compliant key management technology and processes that protect the user's private key. Mechanisms exist to facilitate the implementation of identification and access	5	
		Functional	intersects with	Management (IAM) Identification & Authentication for Organizational Users	IAC-01	wechanisms exist to distinct the imprementation of internit autoria and secess management controls. Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
		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	



FDE II	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		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.	5	
		Functional	intersects with	Identification & Authentication for Third Party Systems & Services	IAC-05	Mechanisms exist to identify and authenticate third-party systems and services.	5	
	The entity implements logical access security software. Infrastructure, and architectures over protected	Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
CC6.1	information assets to protect them from security events to meet the entity's objectives.	Functional	intersects with	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and systems.	5	
		Functional	intersects with	User Identity (ID) Management Authenticator	IAC-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators. Mechanisms exist to securely manage authenticators for users and devices.	5	
		Functional	intersects with	Management Vendor-Supplied Defaults	IAC-10.8	Mechanisms exist to ensure vendor-supplied defaults are changed as part of the installation process.	5	
		Functional	intersects with	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
		Functional	intersects with	Privileged Account Management (PAM) Access Enforcement	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services. Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to	5	
		Functional	intersects with	Least Privilege	IAC-21	the principle of "least privilege." Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with	5	
		Functional	intersects with	Network Security Controls (NSC)	NET-01	organizational business functions. Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
		Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
		Functional	intersects with	Limit Network Connections Data Flow Enforcement –	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its systems. Mechanisms exist to design, implement and review firewall and router configurations to	5	
		Functional	intersects with	Access Control Lists (ACLs)	NET-04	restrict connections between untrusted networks and internal systems. Mechanisms exist to prohibit the direct connection of a sensitive system to an external	5	
		Functional	intersects with	External System Connections	NET-05.1	network without the use of an organization-defined boundary protection device.	5	
		Functional	intersects with	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	
		Functional	intersects with	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	5	
		Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
CC6.1-POF1	Identifies and Manages the inventory of information Assets	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: - Accurately reflects the current systems, applications and services in use; - Identifies authorized software products, including business justification details; - Is at the level of granularity deemed necessary for tracking and reporting; - Includes organization-defined information deemed necessary to achieve effective property accumality; and - Is available for review and audit by designated organizational personnel.	5	
		Functional	intersects with	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties).	5	
		Functional Functional	intersects with subset of	Data & Asset Classification Information Assurance (IA)	DCH-02 IAO-01	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements. Mechanisms exist to facilitate the implementation of cybersecurity & data privacy	5	
CC6.1-POF2	Assesses New Architectures	Functional	intersects with	Operations Assessments	IAO-01	assessment and authoritation controls. Michanisms esti to formally assess the cybensecurity & data privacy controls in systems, applications and services through information Assurance Program (IAP) activities to determine the extent to winhich the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting executed requirements.	5	
		Functional	intersects with	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	5	
		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 cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
		Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
		Functional	intersects with	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
CC6.1-POF3	Restricts Logical Access	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.	5	
		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	
		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.	5	
		Functional	intersects with	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
CC6.1-POF4	Identifies and Authenticates Users	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.	5	
		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	
		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. Mechanisms exist to utilize a Cloud Access Security Broker (CASB), or similar	5	
		Functional	intersects with	Cloud Access Security Broker (CASB)	CLD-11	technology, to provide boundary protection and monitoring functions that both provide access to the cloud and protect the organization from misuse of cloud resources.	5	
CC6.1-POF5	Considers Network Segmentation (macrosegementation)	Functional	intersects with	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC). Mechanisms exist to treat all users and devices as potential threats and prevent access	5	
		Functional	intersects with	Zero Trust Architecture (ZTA)		to data and resources until the users can be properly authenticated and their access <u>authorized</u> . Mechanisms exist to monitor and control communications at the external network	5	
		Functional	intersects with	Boundary Protection Managed Access Control		boundary and at key internal boundaries within the network. Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	5	
				Points Data Flow Enforcement –		Mechanisms exist to design, implement and review firewall and router configurations to		
CC6.1-POF6	Manages Points of Access	Functional	intersects with	Access Control Lists (ACLs) Managed Access Control Points	NET-04 NET-14.3	restrict connections between untrusted networks and internal systems. Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	5	
		Functional	intersects with	System Hardening Through		Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening	5	
		Functional	intersects with	Baseline Configurations Least Functionality	CFG-03	standards. Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
CC6.1-POF7	Restricts Access to Information Assets			Identity & Access		Mechanisms exist to facilitate the implementation of identification and access		
		Functional	intersects with	Management (IAM)	IAC-01	management controls.	5	



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF II	Secure Controls Framework (SCF) Control Description	Strength of Relationship (ontional)	Notes (optional)
		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.	(optional) 5	
		Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
		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.	5	
CC6.1-POF8	Manages Identification and Authentication	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.	5	
		Functional	intersects with	Identification & Authentication for Third Party Systems & Services	IAC-05	Mechanisms exist to identify and authenticate third-party systems and services.	5	
		Functional	intersects with	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
				Identity & Access		Mechanisms exist to facilitate the implementation of identification and access		
CC6.1-POF9	Manages Credentials for Infrastructure and Software	Functional	intersects with	Management (IAM)	IAC-01	management controls.	5	
		Functional	intersects with	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	5	
		Functional	intersects with	Security Authorization	IAO-07	Mechanisms exist to ensure systems, projects and services are officially authorized prior to "go live" in a production environment.	5	
		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	
		Functional	intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
		Functional	intersects with	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
		Functional	intersects with	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest. Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI)	5	
CC6.1-POF10	Uses Encryption to Protect Data	Functional	intersects with	Public Key Infrastructure (PKI)	CRY-08	infrastructure or obtain PKI services from a reputable PKI service provider.	5	
		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	
		Functional	intersects with	Symmetric Keys	CRY-09.1	Mechanisms exist to facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes.	5	
		Functional	intersects with	Asymmetric Keys	CRY-09.2	Mechanisms exist to facilitate the production and management of asymmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes that protect the user's private key.	5	
		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	
		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	
		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	
CC6.1-POF11	Protects Cryptographic Keys	Functional	intersects with	Symmetric Keys	CRY-09.1	Mechanisms exist to facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key	5	
	roccers or programme or to	Functional	intersects with	Asymmetric Keys	CRY-09.2	management technology and processes. Mechanisms exist to facilitate the production and management of asymmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes that protect the user's private key.	5	
		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	
		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	5	
		Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	processes. Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
CC6.1-POF12	Restricts Access to and Use of Confidential Information for Identified Purposes	Functional	intersects with	Access To Sensitive / Regulated Data	IAC-20.1	Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.	5	
		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	
		Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
		Functional	intersects with	Access To Sensitive / Regulated Data	IAC-20.1	Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.	5	
CC6.1-POF13		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	
CC6.1-POF13	Restricts Access to and the Use of Personal Information	Functional	intersects with	Security of Personal Data		Mechanisms exist to ensure Personal Data (PD) is protected by security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	5	
		Functional	intersects with	Internal Use of Personal Data 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: - Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and	5	
						 Authorizes the use of PD when such information is required for internal testing, training and research. Mechanisms exist to utilize a formal user registration and de-registration process that 		
	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal	Functional	intersects with	User Provisioning & De- Provisioning	IAC-07	governs the assignment of access rights. Mechanisms exist to revoke user access rights following changes in personnel roles and	5	
CC6.2	and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Functional	intersects with	Change of Roles & Duties	IAC-07.1	duties, if no longer necessary or permitted. Mechanisms exist to periodically-review the privileges assigned to individuals and	5	
		Functional	intersects with	Periodic Review of Account Privileges	IAC-17	service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	
		Functional	intersects with	User Provisioning & De- Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
CC6.2-POF1	Creates Access Credentials to Protected Information Assets	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.	5	
		Functional	intersects with	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5	
		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.	5	
CC6.2-POF2	Reviews Validity of Access Credentials	Functional	intersects with	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	5	
		Functional	intersects with	System Account Reviews	IAC-15.7	Mechanisms exist to review all system accounts and disable any account that cannot be associated with a business process and owner.	5	
		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	
		Functional	intersects with	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to systems and facilities upon personnel reassignment or transfer, in a timely manner.	5	
		Functional	intersects with	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
CC6.2-POF3	Prevents the Use of Credentials When No Longer Valid	Functional	intersects with	User Provisioning & De- Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights. Mechanisms exist to review all system accounts and disable any account that cannot be	5	
I		Functional	intersects with	System Account Reviews	IAC-15.7	associated with a business process and owner.	5	



## 18	FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
### 1898			Functional	intersects with		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	(optional) 5	
Heales the properties of the components of the c	CC6.3	assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of	Functional	equal	Role-Based Access Control	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for	10	
No. 1 Marchael Annie 1 Marchael 1		least privilege and segregation of duties, to meet the entity's objectives.	Functional	intersects with		IAC-07		5	
Part	CC6.3-POF1	Creates or Modifies Access to Protected Information Assets	Functional	intersects with		IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and	5	
Mathematical part			Functional	intersects with		IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or	5	
## 1987 1997 1997 1997 1997 1997 1997 1997	CC6 3-POF2	Removes Access to Protected Information Assets	Functional	intersects with		IAC-07	governs the assignment of access rights.	5	
1960년 전 1840년 184			Functional	intersects with		IAC-07.1	duties, if no longer necessary or permitted.	5	
Mark Section	CC6.3-POF3	Uses Access Control Structures	Functional	equal		IAC-08	resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	10	
Heave the second	CC6.3-POF4	Reviews Access Roles and Rules	Functional	equal	Periodic Review of Account Privileges	IAC-17	service accounts to validate the need for such privileges and reassign or remove	10	
변경 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			Functional	intersects with	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection	5	
지 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			Functional	intersects with		PES-02	authorized access to organizational facilities (except for those areas within the facility	5	
### 1985	CC6.4	facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's	Functional	intersects with		PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based	5	
1							Physical access control mechanisms exist to enforce physical access authorizations for		
1			Functional	intersects with	Physical Access Control	PES-03	those areas within the facility officially designated as publicly accessible).	5	
지수는 이 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			Functional	intersects with		PES-01		5	
Second Continues (Functional	intersects with		PES-02	authorized access to organizational facilities (except for those areas within the facility	5	
1	CC6.4-POF1	Creates or Modifies Physical Access	Functional	intersects with	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based	5	
Marie Mari			Eunctional	intercepts with	Physical Access Control	DEC 03	all physical access points (including designated entry/exit points) to facilities (excluding		
March Marc			runctional	intersects with		FE3-03		,	
Mathematical Part			Functional	intersects with		PES-01	controls.	5	
Section Part			Functional	intersects with	Visitor Access Revocation	PES-06.6	surrendered before visitors leave the facility or are deactivated at a pre-determined	5	
Part	CC6.4-POF2	Removes Physical Access	Functional	intersects with		PES-02	authorized access to organizational facilities (except for those areas within the facility	5	
Manual M			Functional	intersects with	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	5	
No. 10.00 Procession Proc			Functional	intersects with	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding	5	
Manual M	CCE 4 BOE2	Receiver Bhysical Deuteer	Functional	intersects with	Return of Assets	AST-10	organizational assets in their possession upon termination of employment, contract or	5	
	CC8.470F3	NELOVEIS FITYSILAI DEVILES	Functional	intersects with	Asset Collection	HRS-09.1	Mechanisms exist to retrieve organization-owned assets upon termination of an	5	
Part	CC6.4-POF4	Reviews Physical Access		intersects with			through controlled ingress and egress points.		
Particular Par							security incidents.		
Part Column Part Colum			Functional	subset of		DCH-01	Mechanisms exist to securely dispose of, destroy or repurpose system components	10	
The rest places arrange and place placed and place places and some proposed and serve p			Functional	intersects with		AST-09	using organization-defined techniques and methods to prevent information being recovered from these components.	5	
Processing and principle of processing and principle of the collection one of principle and processing of the processing of the collection one entrolising of the designation or the principle of the principle			Functional	intersects with	Physical Media Disposal	DCH-08	formal procedures.	5	
Procession of Procession with Information Deposed SOP-22 (Authorities well as a company of the procession of the process	CC6.5		Functional	intersects with	System Media Sanitization	DCH-09	commensurate with the classification or sensitivity of the information prior to disposal,	5	
Functional interacts with Protocol Data and Software for Disposed CCS - PGT1 Removes Data and Software for Disposed Functional Interacts with Protocol Data Relations to Protocol Da		objectives.	Functional	intersects with	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5	
Residence Republic Residence R							Retain Personal Data (PD), including metadata, for an organization-defined time		
Miles Mile			Functional	intersects with		PRI-05	Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and	5	
Functional intersects with Personal Control Report Plant Secret Poliposal Control Report Plant Plant Secret Poliposal Control Report Plant Secret Poliposal Control Plant Secret Poliposal Co									
Functional intersects with Processing Media Sentitution Control (Explanation Control (Explana	CC6.5-POF1	Removed from TSC 2017	N/A	N/A		N/A	Mechanisms exist to securely dispose of, destroy or repurpose system components	5	Removed from TSC 2017
Functional intersects with Physical Media Santization DCH ag Functional intersects with Physical Media Santization DCH ag Functional intersects with System Media Santization DCH ag Functional intersects with Information Disposal DCH 20 Functional intersects with Information Disposal DCH 21 Functional intersects with Information Disposal DCH 22 Functional intersects with Information DCH 22 Functional intersects with Informatio			Functional	intersects with		AST-09	recovered from these components.	5	
Punctional intersects with Information Disposal Functional intersects with Personal Data Retention & Per			Functional	intersects with	Physical Media Disposal	DCH-08		5	
Removes Data and Software for Disposal Functional intersects with Information Disposal Disposal Prunctional intersects with Information Disposal D			Europe 1	into	Suction Made to 1	DC::	commensurate with the classification or sensitivity of the information prior to disposal,		
Functional intersects with Personal Data Retention & Disposal Personal Data Retention Reten	CC6.5-POF2	Removes Data and Software for Disposal	runctional	intersects with	system Media Sanitization	DCH-09	release out of organizational control or release for reuse.	5	
Functional intersects with Personal Data Retention & Disposal of self-interpretation of building mentatables, for an organization defined time personal to fulfill the purpose; islamined inter notice or a required by law, "Dispose of, destroys, erakes, and/or anonymizes the PD, regardless of the method of song; and "Live organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and architecteroscipes). In the control of PD (including originals, copies and architecteroscipes). In the control of PD (including originals, copies and architecteroscipes). In the control of PD (including originals, copies and architecteroscipes). In the control of PD (including originals, copies and architecteroscipes). In the control of PD (including originals, copies and architecteroscipes and including emethod of song; and "Live originalization-defined time period to fulfill the purpose; objects and architecteroscipes and including emethod of song; and control to fulfill the purpose; islamined in the notice or a requirement of the motion or a live originalization-defined time period to fulfill the purpose; islamined in the notice or a requirement of the notice or a requirement or a "Live originalization-defined techniques or method of song; and "Live originalization-defined techniques or method or definition or definition or definition or defini			Functional	intersects with	Information Disposal	DCH-21		5	
Personal for a Recention & Dispose of, destroys, erakes, and/or anonymizes the Ppt, regardless of the method of sorge; and - use organization-effend etechniques or methods to ensure secure deletion or destruction of Ppt (including originals, copies and archived records). Functional intersects with							Retain Personal Data (PD), including metadata, for an organization-defined time		
Functional intersects with Functional intersects			Functional	intersects with		PRI-05	 Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and 	5	
Functional intersects with functional intersects							destruction of PD (including originals, copies and archived records).		
Functional intersects with Functional intersects with Prunctional intersects with Functional Functional intersects with Functional Functi			Functional	intersects with	Management (IAM)	IAC-01	management controls.	5	
Functional Intersects with (NEC) NET-02 Implementation of Network Section of Ne			Functional	intersects with	and Audit (AAA)	IAC-01.2	solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
Functional intersects with Layered Network Defenses NET-Q2 interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers on the functional on the functional on the function and corrid communications at the external network. Mechanisms exist to monitor and corrid communications at the external network on the external network of t			Functional	intersects with	Network Security Controls (NSC)	NET-01	implementation of Network Security Controls (NSC). Mechanisms exist to implement security functions as a layered structure that minimizes	5	
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries. The entity implements logical access security measures to protect against threats from sources outside its system boundaries. The entity implements logical access security measures to protect against threats from sources outside its system. Functional intersects with Limit Network Connections NET-03.1.8 its systems. Data Flow Enforcement - Data Flow Enforcement - NET-04 its systems. Data Flow Enforcement - NET-05 its systems - NET-05			Functional	intersects with	Layered Network Defenses	NET-02	on the functionality or correctness of higher layers.	5	
The entity implements logical access security measures to protect against threats from sources outside its system boundaries. The entity implements logical access security measures to protect against threats from sources outside its system Functional intersects with Data Flow Enforcement - Access Control Lists (ACLS) Deny Traffic by Default & Mechanisms exist to design, implement and review frewall and router configurations to destruct connections between untrusted networks and internal systems. 5 Mechanisms exist to configure firewall and router configurations to deny network traffic							boundary and at key internal boundaries within the network.		
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries. Functional intersects with functional intersects with access Control Lists (ACLs) NET-04 restrict connections between untrusted networks and internal systems. 5 Access Control Lists (ACLs) Net-04 restrict connections between untrusted networks and internal systems. 5 Deny Traffic by Default & Deny Traffic by Den							its systems. Mechanisms exist to design, implement and review firewall and router configurations to	5	
Deny Traffic by Default & NET Of A by Africa by Afri	CC6.6		Functional	intersects with	Access Control Lists (ACLs)	NET-04	· ·	5	
			Functional	intersects with	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1		5	



FDE#	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF II	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
		Functional	intersects with	DMZ Networks Safeguarding Data Over	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks. Cryptographic mechanisms exist to implement strong cryptography and security	5	
		Functional	intersects with	Open Networks	NET-12	protocols to safeguard sensitive/regulated data during transmission over open, public networks. Mechanisms exist to protect external and internal wireless links from signal parameter	5	
		Functional	intersects with	Wireless Link Protection	NET-12.1	attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered.	5	
		Functional	intersects with	Electronic Messaging Remote Access	NET-13 NET-14	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications. Mechanisms exist to define, control and review organization-approved, secure remote	5	
		Functional	intersects with	Network Security Controls (NSC)	NET-01	access methods. Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
CC6.6-POF1	Restricts Access	Functional	intersects with	Boundary Protection Data Flow Enforcement –	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network. Mechanisms exist to design, implement and review firewall and router configurations to	5	
		Functional	intersects with	Access Control Lists (ACLs)	NET-04	restrict connections between untrusted networks and internal systems. Mechanisms exist to configure firewall and router configurations to deny network traffic	5	
		Functional	intersects with	Allow Traffic by Exception Use of Cryptographic		by default and allow network traffic by exception (e.g., deny all, permit by exception). Mechanisms exist to facilitate the implementation of cryptographic protections controls	5	
		Functional	intersects with	Controls Identity & Access	CRY-01 IAC-01	using known public standards and trusted cryptographic technologies. Mechanisms exist to facilitate the implementation of identification and access	5	
		Functional	intersects with	Management (IAM) Authenticate, Authorize and Audit (AAA)		management controls. Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
CC6.6-POF2	Protects Identification and Authentication Credentials	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	
		Functional	intersects with	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC). Cryptographic mechanisms exist to implement strong cryptography and security	5	
		Functional	intersects with	Safeguarding Data Over Open Networks		protocols to safeguard sensitive/regulated data during transmission over open, public networks. Mechanisms exist to protect the confidentiality, integrity and availability of electronic	5	
		Functional	intersects with	Electronic Messaging Identity & Access Management (IAM)	NET-13 IAC-01	messaging communications. Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
		Functional	intersects with	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
		Functional	intersects with	Multi-Factor	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: Remote network access; -Third-party systems, applications and/or services; and/or	5	
CC6.6-POF3	Requires Additional Authentication or Credentials	runctional	intersects with	Authentication (MFA) Adaptive Identification &	IAC-00	Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data. Mechanisms exist to allow individuals to utilize alternative methods of authentication		
CC0.0+0r3	nequires Auditional Authoritication of Cleventians	Functional	intersects with	Authentication Network Security Controls	IAC-13 NET-01	under specific circumstances or situations. Mechanisms exist to develop, govern & update procedures to facilitate the	5	
		Functional	intersects with	(NSC) Boundary Protection	NET-03	implementation of Network Security Controls (NSC). Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
		Functional	intersects with	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
		Functional	intersects with	Remote Access Network Security Controls	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods. Mechanisms exist to develop, govern & update procedures to facilitate the	5	
		Functional	intersects with	(NSC)	NET-01	implementation of Network Security Controls (NSC). Mechanisms exist to implement security functions as a layered structure that minimizes	5	
CC6.6-POF4	Implements Boundary Protection Systems	Functional	intersects with	Layered Network Defenses	NET-02	interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	5	
		Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
		Functional	intersects with	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	5	
		Functional	intersects with	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	5	
		Functional	intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
		Functional	intersects with	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
		Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
		Functional	intersects with	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
		Functional	intersects with	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Functional	intersects with	Use of External Information Systems	DCH-13	Mechanisms exist to govern how external parties, systems and services are used to securely store, process and transmit data.	5	
		Functional	intersects with	Portable Storage Devices		Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
		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.	5	
		Functional	intersects with	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	5	
		Functional	intersects with	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	5	
		Functional	intersects with	Full Device & Container- Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	5	
		Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
		Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening	5	
		Functional	intersects with	Least Functionality	CFG-03	standards. Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
	Subject to Addition to Subject Township	Functional	intersects with	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	5	
CC6.7-POF1	Restricts the Ability to Perform Transmission	Functional	intersects with	Prevent Unauthorized Exfiltration Deny Traffic by Default &	NET-03.5	Automated mechanisms exist to prevent the unauthorized exfiltration of sensitive/regulated data across managed interfaces. Mechanisms exist to configure firewall and router configurations to deny network traffic	5	
		Functional	intersects with	Allow Traffic by Exception End-User Messaging	NET-04.1 NET-12.2	by default and allow network traffic by exception (e.g., deny all, permit by exception). Mechanisms exist to prohibit the transmission of unprotected sensitive/regulated data	5	
		Functional	intersects with	Technologies Data Loss Prevention (DLP)	NET-17	by end-user messaging technologies. Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
		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	
ccc 7 0	Hore Execution Technologies or Secure Commission - Commis	Functional	intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
CC6.7-POF2	Uses Encryption Technologies or Secure Communication Channels to Protect Data	Functional	intersects with	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
		Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
						•		



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (ontional)	Notes (optional)
		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	
		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	
CC6.7-POF3	Protects Removal Media	Functional	intersects with	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards. Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
CC0.7 1 013	TOCCO TOTAL MODE	Functional	intersects with	Encrypting Data At Rest Storage Media	CRY-05 CRY-05.1	Cryptographic mechanisms exist to protect the confidentiality and integrity of	5	
		Functional	equal	Removable Media Security	DCH-12	sensitive/regulated data residing on storage media. Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	10	
		Functional	intersects with	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems. Mechanisms exist to facilitate the implementation of endpoint security controls.	5	
CC6.7-POF4	Protects Endpoint Devices	Functional	intersects with	Endpoint Security Centralized Management	END-01 MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM)	5	
		Functional	intersects with	Of Mobile Devices Prohibition Of Changes	CHG-02.1	controls. Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	5	
		Functional	intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
		Functional	intersects with	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5	
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized	F		Host Intrusion Detection	FND 07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host	5	
CC0.8	The entry implements controls to prevent or detect and act upon the introduction of disautionized	Functional	intersects with	and Prevention Systems (HIDS / HIPS)	END-07	activity, including lateral movement across the network Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection	,	
		Functional	intersects with	File Integrity Monitoring (FIM)	MON-01.7	technology, on critical assets to generate alerts for unauthorized modifications.	5	
		Functional	intersects with	Boundary Protection Network Intrusion	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network. Mechanisms exist to employ Network Intrusion Detection / Prevention Systems	5	
		Functional	intersects with	Detection / Prevention Systems (NIDS / NIPS)	NET-08	(NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	
		Functional	intersects with	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	
				Restrict Roles Permitted To		Mechanisms exist to configure systems to prevent the installation of software, unless the action is performed by a privileged user or service.		
CC6.8-POF1	Restricts Installation and Modification of Application and Software	Functional	intersects with	Install Software	CFG-05.2		5	
		Functional	intersects with	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	
		Functional	intersects with	Unauthorized Installation	CFG-05.1	Mechanisms exist to configure systems to generate an alert when the unauthorized installation of software is detected.	5	
CC6.8-POF2	Detects Unauthorized Changes to Software and Configuration Parameters			Alerts		Mechanisms exist to generate an alert when new software is detected.		
		Functional	intersects with	Software Installation Alerts Change Management	END-03.1 CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
CC6.8-POF3	Uses a Defined Change Control Process	Functional	intersects with	Program Configuration Change Control	CHG-01	Mechanisms exist to govern the technical configuration change control processes.	5	
CC6.8-POF4	Uses Antivirus and Anti-Malware Software	Functional	equal	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	
						Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically		
CC6.8-POF5	Scans Information Assets From Outside the Entity for Malware and Other Unauthorized Software	Functional	equal	Always On Protection	END-04.7	authorized by management on a case-by-case basis for a limited time period.	10	
		Functional	intersects with	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	5	
		Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Functional	intersects with	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	5	
	Vallet de la lace	Functional	intersects with	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical assets to generate alerts for unauthorized modifications.	5	
		Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
		Functional	intersects with	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	5	
CC7.1-POF1	Uses Defined Configuration Standards	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening	5	
		Functional	intersects with	Automated Central Management &	CFG-02.2	standards. Automated mechanisms exist to govern and report on baseline configurations of systems through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
				Verification Endpoint File Integrity		Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to		
CC7.1-POF2	Monitors Infrastructure and Software	Functional	intersects with	Monitoring (FIM) File Integrity Monitoring		detect and report on unauthorized changes to selected files and configuration settings. Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection	5	
		Functional	intersects with	(FIM)		technology, on critical assets to generate alerts for unauthorized modifications. Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to	5	
CC7.1-POF3	Implements Change-Detection Mechanisms	Functional	intersects with	Endpoint File Integrity Monitoring (FIM)	END-06	detect and report on unauthorized changes to selected files and configuration settings. Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection	5	
		Functional	intersects with	File Integrity Monitoring (FIM)	MON-01.7	technology, on critical assets to generate alerts for unauthorized modifications.	5	
		Functional	intersects with	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components. Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to	5	
CC7.1-POF4	Detects Unknown or Unauthorized Components	Functional	intersects with	Endpoint File Integrity Monitoring (FIM)	END-06	detect and report on unauthorized changes to selected files and configuration settings.	5	
		Functional	intersects with	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical assets to generate alerts for unauthorized modifications.	5	
CC7.1-POF5	Conducts Vulnerability Scans	Functional	equal	Vulnerability Scanning Automated Central	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. Automated mechanisms exist to govern and report on baseline configurations of	10	
		Functional	intersects with	Management & Verification	CFG-02.2	systems through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
		Functional	intersects with	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
		Functional	intersects with	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
		Functional	intersects with	Automated Tools for Real- Time Analysis	MON-01.2	Mechanisms exist to utilize a Security incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
		Functional	intersects with	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	
		Functional	intersects with	System Generated Alerts	MON-01 4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational	5	
				Wireless Intrusion		awareness. Mechanisms exist to utilize Wireless Intrusion Detection / Protection Systems (WIDS /		
		Functional	intersects with	Detection System (WIDS)	MON-01.5	WIPS) to identify rogue wireless devices and to detect attack attempts via wireless networks. Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS	5	
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are	Functional	intersects with	Host-Based Devices	MON-01.6	/ HIPS) to actively alert on or block unwanted activities and send logs to a Security Incident Event Manager (SIEM), or similar automated tool, to maintain situational awareness.	5	
·· -	analyzed to determine whether they represent security events.	Functional	intersects with	Reviews & Updates	MON-01.8	awareness. Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
	1		l	l	L	<u> </u>	l	1



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
				Centralized Collection of	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	(optional) 5	
		Functional	intersects with	Security Event Logs Correlate Monitoring	MON-02.1	automated tool, to support the centralized collection of security-related event logs. Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar	5	
				Information		automated tool, to enhance organization-wide situational awareness. Mechanisms exist to provide an event log report generation capability to aid in		
		Functional	intersects with	Monitoring Reporting	MON-06	detecting and assessing anomalous activities. Mechanisms exist to detect and respond to anomalous behavior that could indicate	5	
		Functional	intersects with	Anomalous Behavior	MON-16	account compromise or other malicious activities.	5	
		Functional	intersects with	Security Concept Of Operations (CONOPS)	OPS-02	Mechanisms exist to develop a security Concept of Operations (CONOPS), or a similarly- defined plan for achieving cybersecurity objectives, that documents management, operational and technical measures implemented to apply defense-in-depth techniques that is communicated to all appropriate stakeholders.	5	
		Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
		Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
		Functional	intersects with	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
CC7.2-POF1	Implements Detection Policies, Procedures, and Tools	Functional	intersects with	Automated Tools for Real- Time Analysis	MON-01.2	Mechanisms exist to utilize a Security incident Event Manager (SEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
		Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	5	
		Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
		Functional	intersects with	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
		Functional	intersects with	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	
CC7.2-POF2	Designs Detection Measures	Functional	intersects with	Automated Alerts	MON- 01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	5	
		Functional	intersects with	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
		Functional	intersects with	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
CC7.2-POF3	Implements Filters to Analyze Anomalies	Functional	intersects with	Automated Tools for Real- Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
		Functional	intersects with	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
CC7.2-POF4	Monitors Detection Tools for Effective Operation	Functional	intersects with	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	
		Functional	intersects with	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
		Functional	intersects with	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents. Mechanisms exist to implement and govern processes and documentation to facilitate	5	
		Functional	intersects with	Incident Response Operations	IRO-01	an organization-wide response capability for cybersecurity & data privacy-related incidents.	5	
		Functional	intersects with	Incident Handling Incident Response Plan	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery. Mechanisms exist to maintain and make available a current and viable incident	5	
		Functional	intersects with	(IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable incident Response Plan (IRP) to all stakeholders. Mechanisms exist to address data breaches, or other incidents involving the	5	
		Functional	intersects with	Data Breach	IRO-04.1	unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations. Machanisms system utility a Security Incident Event Manager (SIEM) or similar.	5	
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	automated tool, to support the centralized collection of security-related event logs.	5	
		Functional	intersects with	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
		Functional	intersects with	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	
		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 systems and data.	5	
		Functional	intersects with	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	
		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 & data privacy-related incidents.	5	
CC7.3-POF1	Responds to Security Incidents	Functional	intersects with	Incident Handling Incident Response Plan	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery. Mechanisms exist to maintain and make available a current and viable incident	5	
-		Functional	intersects with	(IRP) Situational Awareness For	IRO-04	Response Plan (IRP) to all stakeholders. Mechanisms exist to document, monitor and report the status of cybersecurity & data	5	
CC7.3-POF2	Communicates and Reviews Detected Security Events	Functional	intersects with	Incidents Incident Stakeholder	IRO-09	privacy incidents to internal stakeholders all the way through the resolution of the incident. Mechanisms exist to timely-report incidents to applicable: Internal stakeholders;	5	
	• • • • • • • • • • • • • • • • • • • •	Functional	intersects with	Reporting Cyber Incident Reporting	IRO-10.2	Affected clients & third-parties; and Regulatory authorities. Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
CC7.3-POF3	Develops and Implements Procedures to Analyze Security Incidents		subset of	for Sensitive Data Incident Handling	IRO-10.2	Mechanisms exist to cover the preparation, automated detection or intake of incident	10	
CC7.3-POF3	Develops and implements Procedures to Analyze Security Incidents	Functional	subset of intersects with	Incident Handling Incident Handling	IRO-02	reporting, analysis, containment, eradication and recovery. Mechanisms exist to cover the preparation, automated detection or intake of incident	5	
CC7.3-POF4	Assesses the Impact on Confidential Information	Functional	intersects with	Data Breach	IRO-04.1	reporting, analysis, containment, eradication and recovery. Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws,	5	
		Functional	intersects with	Incident Handling	IRO-04.1	unautionized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations. Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
CC7.3-POF5	Determines Confidential Information Used or Disclosed	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,	5	
		Functional	intersects with	Incident Handling	IRO-02	regulations and contractual obligations. Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
	l							



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
CC7.3-POF6	Assesses the Impact on Personal Information					Mechanisms exist to identify: Assumptions affecting risk assessments, risk response and risk monitoring;	(optional)	
		Functional	intersects with	Risk Framing	RSK-01.1	Constraints affecting risk assessments, risk response and risk monitoring; The organizational risk tolerance; and Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
		Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
CC7.3-POF7	Determines Personal Information Used or Disclosed	Functional	intersects with	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5	
		Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
		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 & data privacy-related	5	
		Functional	intersects with	Incident Handling	IRO-02	incidents. Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
		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.	5	
		Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
		Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	5	
CC7.4	The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Functional	intersects with	Incident Stakeholder	IRO-10	Mechanisms exist to timely-report incidents to applicable: Internal stakeholders;	5	
		Functional	intersects with	Reporting Cyber Incident Reporting for Sensitive Data	IRO-10.2	Affected clients & third-parties; and Regulatory authorities. Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
						Mechanisms exist to provide cybersecurity & data privacy incident information to the provider of the product or service and other organizations involved in the supply chain		
		Functional	intersects with	Supply Chain Coordination	IRO-10.4	for systems or system components related to the incident.	5	
		Functional	intersects with	Coordination With External Providers Regulatory & Law	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers. Mechanisms exist to maintain incident response contacts with applicable regulatory	5	
		Functional	intersects with	Enforcement Contacts Risk Remediation	IRO-14 RSK-06	and law enforcement agencies. Mechanisms exist to remediate risks to an acceptable level.	5	
						Mechanisms exist to define cybersecurity responsibilities for all personnel.		
		Functional	intersects with	Roles & Responsibilities Incident Response	HRS-03	Mechanisms exist to implement and govern processes and documentation to facilitate	5	
		Functional	intersects with	Operations	IRO-01	an organization-wide response capability for cybersecurity & data privacy-related incidents. Mechanisms exist to cover the preparation, automated detection or intake of incident	5	
CC7.4-POF1	Assigns Roles and Responsibilities	Functional	intersects with	Incident Handling	IRO-02	reporting, analysis, containment, eradication and recovery.	5	
		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.	5	
		Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
		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 & data privacy-related	5	
CC7.4-POF2	Contains and Responds to Security Incidents	Functional	intersects with	Incident Handling	IRO-02	Incidents. Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
		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.	5	
		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 & data privacy-related incidents.	5	
CC7.4-POF3	Mittigates Ongoing Security Incidents	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
		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. Mechanisms exist to implement and govern processes and documentation to facilitate	5	
CC7.4-POF4	Resolves Security Incidents	Functional	intersects with	Incident Response Operations	IRO-01	an organization-wide response capability for cybersecurity & data privacy-related incidents.	5	
CC7.4-FOF4	RESURES SECURITY INCIDENTS	Functional	intersects with	Incident Handling Incident Response Plan	IRO-02 IRO-04	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery. Mechanisms exist to maintain and make available a current and viable incident	5	
		Functional	intersects with	(IRP) Business Continuity	IRO-04	Response Plan (IRP) to all stakeholders. Mechanisms exist to facilitate the implementation of contingency planning controls to	5	
		Functional	intersects with	Management System (BCMS)	BCD-01	help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
CC7.4-POF5	Restores Operations	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 & data privacy-related incidents.	5	
		Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
		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. Mechanisms exist to implement and govern processes and documentation to facilitate	5	
		Functional	intersects with	Incident Response Operations	IRO-01	an organization-wide response capability for cybersecurity & data privacy-related incidents.	5	
		Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
		Functional	intersects with	Incident Response Plan (IRP)		Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
CC7.4-POF6	Develops and Implements Communication of Security Incidents	Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the	5	
		Functional	intersects with	Incident Stakeholder	IRO-10	incident. Mechanisms exist to timely-report incidents to applicable: Internal stakeholders;	5	
				Reporting		Affected clients & third-parties; and Regulatory authorities. Mechanisms exist to report sensitive/regulated data incidents in a timely manner.		
		Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to implement and govern processes and documentation to facilitate	5	
		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 & data privacy-related incidents.	5	
						Mechanisms exist to cover the preparation, automated detection or intake of incident		
CC7.4-POF7	Obtains Understanding of Nature of Incident and Determines Containment Strategy	Functional	intersects with	Incident Handling	IRO-02	reporting, analysis, containment, eradication and recovery.	5	
						Mechanisms exist to maintain and make available a current and viable Incident		
		Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Response Plan (IRP) to all stakeholders.	5	
		Functional	intersects with	Incident Response	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related	5	
		Functional	intersects with	Operations Incident Handling	IRO-01	incidents. Mechanisms exist to cover the preparation, automated detection or intake of incident	5	
CC7.4-POF8	Remediates Identified Vulnerabilities	Functional	intersects with	Incident Response Plan	IRO-02 IRO-04	reporting, analysis, containment, eradication and recovery. Mechanisms exist to maintain and make available a current and viable Incident	5	
		Functional	intersects with	(IRP) Risk Remediation	RSK-06	Response Plan (IRP) to all stakeholders. Mechanisms exist to remediate risks to an acceptable level.	5	
		Functional	intersects with	Vulnerability Remediation	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and	5	
		Functional	intersects with	Process Incident Response	IRO-01	remediated. Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related	5	
		Functional	intersects with	Operations Incident Handling	IRO-02	incidents. Mechanisms exist to cover the preparation, automated detection or intake of incident	5	
		Functional	intersects with	Incident Response Plan (IRP)	IRO-02	reporting, analysis, containment, eradication and recovery. Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
CC7 4-POF9	Communicates Remediation Activities		1	(ove)		Transporter Cont (100 / 100 MH attentional de	1	1



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (ontional)	Notes (optional)
CC/-41 O/3	eminomenes nemediation victories	Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	(optional) 5	
		Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: Internal stakeholders; Affected clients & third-parties; and	5	
		Functional	intersects with	Contingency Plan Root Cause Analysis (RCA) &	BCD-05	 Regulatory authorities. Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated. 	5	
		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 & data privacy-related	5	
CC7.4-POF10	Evaluates the Effectiveness of incident Response	Functional	intersects with	Incident Handling	IRO-02	incidents. Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
		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. Mechanisms exist to incorporate lessons learned from analyzing and resolving	5	
		Functional	intersects with	Root Cause Analysis (RCA) & Lessons Learned Incident Response	IRO-13	cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents. Mechanisms exist to implement and govern processes and documentation to facilitate	5	
		Functional	intersects with	Operations	IRO-01	an organization-wide response capability for cybersecurity & data privacy-related incidents. Mechanisms exist to cover the preparation, automated detection or intake of incident	5	
CC7.4-POF11	Periodically Evaluates incidents	Functional	intersects with	Incident Handling Incident Response Plan		reporting, analysis, containment, eradication and recovery. Mechanisms exist to maintain and make available a current and viable Incident	5	
		Functional	intersects with	(IRP)		Response Plan (IRP) to all stakeholders. Mechanisms exist to regularly review and modify incident response practices to	5	
		Functional	intersects with	IRP Update Incident Response	IRO-04.2	incorporate lessons learned, business process changes and industry developments, as necessary. Mechanisms exist to implement and govern processes and documentation to facilitate	5	
CC7.4-POF12	Applies Breach Response Procedures	Functional	intersects with	Operations	IRO-01	an organization-wide response capability for cybersecurity & data privacy-related incidents. Mechanisms exist to cover the preparation, automated detection or intake of incident	5	
		Functional	intersects with	Incident Handling Incident Response Plan (IRP)	IRO-04	reporting, analysis, containment, eradication and recovery. Mechanisms exist to maintain and make available a current and viable incident Response Plan (IRP) to all stakeholders.	5	
		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 & data privacy-related incidents.	5	
		Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
CC7.4-POF13	Communicates Unauthorized Use and Disclosure	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.	5	
		Functional	intersects with	Incident Stakeholder	IRO-10	Mechanisms exist to timely-report incidents to applicable: Internal stakeholders; Mifortal cliants & third-parties: and	5	
		Functional	intersects with	Reporting Cyber Incident Reporting	IRO-10.2	Affected clients & third-parties; and Regulatory authorities. Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
CC7.4-POF14	Application of Sanctions	Functional	subset of	for Sensitive Data Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security	10	
		Functional	intersects with	Business Continuity Management System	BCD-01	policies, standards and procedures. Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or	5	
		Functional	intersects with	(BCMS) Identify Critical Assets	BCD-02	Business Continuity & Disaster Recovery (BC/DR) playbooks). Mechanisms exist to identify and document the critical systems, applications and	5	
		Functional	intersects with	Resume All Missions & Business Functions	BCD-02.1	services that support essential missions and business functions. Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	5	
		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.	5	
		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.	5	
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	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.	5	
		Functional	intersects with	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
		Functional	intersects with	Contingency Planning & Updates	BCD-06	Mechanisms exist to keep contingency plans current with business needs, technology changes and feedback from contingency plan testing activities. Mechanisms exist to create recurring backups of data, software and/or system images,	5	
		Functional	intersects with	Data Backups	BCD-11	as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
		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. Mechanisms exist to ensure the secure recovery and reconstitution of systems to a	5	
		Functional	intersects with	Information System Recovery & Reconstitution Backup & Restoration	BCD-12	known state after a disruption, compromise or failure. Mechanisms exist to protect backup and restoration hardware and software.	5	
		Functional	intersects with	Hardware Protection Business Continuity	BCD-13	Mechanisms exist to facilitate the implementation of contingency planning controls to	5	
		Functional	subset of	Management System (BCMS)	BCD-01	help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks). Mechanisms exist to resume all missions and business functions within Recovery Time	10	
		Functional	intersects with	Resume All Missions & Business Functions	BCD-02.1	Objectives (RTOs) of the contingency plan's activation.	5	
CC7.5-POF1	Restores the Affected Environment	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.	5	
		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.	5	
		Functional	intersects with	Information System Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of systems to a known state after a disruption, compromise or failure.	5	
		Functional	equal	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
CC7.5-POF2	Communicates Information About the Incident	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	
		Functional	intersects with	Incident Stakeholder	IRO-10	Mechanisms exist to timely-report incidents to applicable: Internal stakeholders;	5	
	Determines Root Cause of the Incident			Reporting Contingency Plan Root		Affected clients & third-parties; and Regulatory authorities. Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity		
CC7.5-POF3	Determines woor cause of the incident	Functional	equal	Cause Analysis (RCA) & Lessons Learned Business Continuity	BCD-05	every time the contingency plan is activated. Mechanisms exist to facilitate the implementation of contingency planning controls to	10	
CC7.5-POF4	Implements Changes to Prevent and Detect Recurrences	Functional	intersects with	Management System (BCMS)	BCD-01	help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
		Functional	intersects with	Contingency Planning & Updates Business Continuity	BCD-06	Mechanisms exist to keep contingency plans current with business needs, technology changes and feedback from contingency plan testing activities. Mechanisms exist to facilitate the implementation of contingency planning controls to	5	
CC7.5-POF5	Improves Response and Recovery Procedures	Functional	intersects with	Management System (BCMS)	BCD-01	help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
		Functional	intersects with	Contingency Planning & Updates Contingency Plan Testing &	BCD-06	Mechanisms exist to keep contingency plans current with business needs, technology changes and feedback from contingency plan testing activities. Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's	5	
CC7.5-POF6	Implements Incident-Recovery Plan Testing	Functional	subset of	Exercises System Hardening Through	BCD-04	effectiveness and the organization's readiness to execute the plan. Mechanisms exist to develop, document and maintain secure baseline configurations	10	
		Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	for technology platforms that are consistent with industry-accepted system hardening standards. Mechanisms exist to review and update baseline configurations:	5	
		Functional	intersects with	Reviews & Updates	CFG-02.1	At least annually; When required due to so; or As part of system component installations and upgrades.	5	



FDE#	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (ontional)	Notes (optional)
		Functional	intersects with	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of systems through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Functional	intersects with	Change Management Program Configuration Change	CHG-01	Mechanisms exist to facilitate the implementation of a change management program. Mechanisms exist to govern the technical configuration change control processes.	5	
		Functional	intersects with	Control Test, Validate & Document	CHG-02	Mechanisms exist to appropriately test and document proposed changes in a non- production environment before changes are implemented in a production	5	
		Functional	intersects with	Changes Stakeholder Notification of	CHG-05	environment. Mechanisms exist to ensure stakeholders are made aware of and understand the	5	
		Functional	intersects with	Changes Secure Development Life Cycle (SDLC) Management	PRM-07	impact of proposed changes. Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
		Functional	intersects with	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
CC8.1-POF1	Manages Changes Throughout the System Life Cycle	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
		Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
		Functional	intersects with	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
CC8.1-POF2	Authorizes Changes	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes. Mechanisms exist to prohibit unauthorized changes, unless organization-approved	5	
		Functional	intersects with	Prohibition Of Changes Access Restriction For Change	CHG-02.1 CHG-04	change requests are received. Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
		Functional	intersects with	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
CC8.1-POF3	Designs and Develops Changes	Functional	intersects with	Configuration Change Control Cybersecurity & Data	CHG-02	Mechanisms exist to govern the technical configuration change control processes. Mechanisms exist to include a cybersecurity and/or data privacy representative in the	5	
		Functional	intersects with	Privacy Representative for Asset Lifecycle Changes	CHG-02.3	configuration change control review process.	5	
		Functional	intersects with	Security Impact Analysis for Changes Change Management	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change. Mechanisms exist to facilitate the implementation of a change management program.	5	
CC8.1-POF4	Documents Changes	Functional	intersects with	Program Configuration Change Control	CHG-01 CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
		Functional	intersects with	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non- production environment before changes are implemented in a production	5	
		Functional	intersects with	Change Management Program	CHG-01	environment. Mechanisms exist to facilitate the implementation of a change management program.	5	
CC8.1-POF5	Tracks System Changes	Functional	intersects with	Configuration Change Control Test. Validate & Document	CHG-02	Mechanisms exist to govern the technical configuration change control processes. Mechanisms exist to appropriately test and document proposed changes in a non-	5	
		Functional	intersects with	Changes Change Management	CHG-02.2	production environment before changes are implemented in a production environment. Mechanisms exist to facilitate the implementation of a change management program.	5	
		Functional	intersects with	Program Configuration Change Control	CHG-01 CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
CC8.1-POF6	Configures Software	Functional	intersects with	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	5	
		Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
		Functional	intersects with	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of systems through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
		Functional	intersects with	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
CC8.1-POF7	Tests System Changes	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
		Functional	intersects with	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non- production environment before changes are implemented in a production environment.	5	
CC8.1-POF8	Approves System Changes	Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program. Mechanisms exist to govern the technical configuration change control processes.	10	
		Functional	subset of	Configuration Change Control Change Management	CHG-02	Mechanisms exist to govern the technical configuration change control processes. Mechanisms exist to facilitate the implementation of a change management program.	10	
		Functional	intersects with	Program Configuration Change	CHG-01	Mechanisms exist to govern the technical configuration change control processes.	5	
CC8.1-POF9	Deploys System Changes	Functional	intersects with	Control Access Restriction For		Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability	5	
		Functional	intersects with	Change Permissions To Implement		of users to conduct unauthorized changes. Mechanisms exist to limit operational privileges for implementing changes.	5	
		Functional	intersects with	Changes Change Management	CHG-04.4 CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
		Functional	intersects with	Program Configuration Change	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
CC8 1-POF10	Identifies and Evaluates System Changes	Functional		Control Test, Validate & Document		Mechanisms exist to appropriately test and document proposed changes in a non-	5	
ccd.1-POF10	Transport of the state of the s		intersects with	Changes Security Impact Analysis		production environment before changes are implemented in a production environment. Mechanisms exist to analyze proposed changes for potential security impacts, prior to		
		Functional	intersects with	for Changes Automated Access		the implementation of the change. Mechanisms exist to perform after-the-fact reviews of configuration change logs to	5	
		Functional	intersects with	Enforcement / Auditing Change Management		discover any unauthorized changes. Mechanisms exist to facilitate the implementation of a change management program.	5	
		Functional	intersects with	Program	CHG-01	Mechanisms exist to govern the technical configuration change control processes.	5	
CC8.1-POF11	Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to perform after-the-fact reviews of configuration change logs to	5	
		Functional	intersects with	Automated Access Enforcement / Auditing Automated Central	CHG-04.1	discover any unauthorized changes. Automated mechanisms exist to govern and report on baseline configurations of	5	
		Functional	intersects with	Management & Verification		systems through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
CC8.1-POF12	Creates Baseline Configuration of IT Technology	Functional	intersects with	Configuration Management Program System Hardening Through	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls. Mechanisms exist to develop, document and maintain secure baseline configurations	5	
		Functional	intersects with	Baseline Configurations Change Management	CFG-02	for technology platforms that are consistent with industry-accepted system hardening standards. Mechanisms exist to facilitate the implementation of a change management program.	5	
		Functional	intersects with	Program	CHG-01	Mechanisms exist to govern the technical configuration change control processes.	5	
CC8.1-POF13	Provides for Changes Necessary in Emergency Situations	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to appropriately test and document proposed changes in a non-	5	
		Functional	intersects with	Test, Validate & Document Changes	CHG-02.2	production environment before changes are implemented in a production environment. Mechanisms exist to establish and control "emergency access only" accounts.	5	
		Functional	intersects with	Emergency Accounts	IAC-15.9		5	
		Functional Functional	intersects with	Change Management Program Configuration Change	CHG-01 CHG-02	Mechanisms exist to facilitate the implementation of a change management program. Mechanisms exist to govern the technical configuration change control processes.	5	
	I	- uncooldi	mucraecta With	Control	Crig-U2			



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
CC8.1-POF14	Manages Patch Changes	Functional	intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
		Functional	intersects with	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	5	
		Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
CC8.1-POF15	Considers System Resilience	Functional	intersects with	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services. Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
		Functional	intersects with	Achieving Resilience Requirements	SEA-01.2		5	
		Functional	intersects with	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
		Functional	intersects with	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non- production environment before changes are implemented in a production environment. Mechanisms exist to facilitate the implementation of data protection controls.	5	
CC8.1-POF16	Protects Confidential Information	Functional	intersects with	Data Protection Vulnerability & Patch	DCH-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability	5	
		Functional	intersects with	Management Program (VPMP) Software & Firmware	VPM-01	management controls. Mechanisms exist to conduct software patching for all deployed operating systems,	5	
		Functional	intersects with	Patching	VPM-05	applications and firmware. Mechanisms exist to facilitate the implementation of data protection controls.	5	
		Functional	intersects with	Data Protection Sensitive / Regulated Data	DCH-01	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
CC8.1-POF17	Protects Personal Information	Functional	intersects with	Protection	DCH-01.2	Mechanisms exist to facilitate the implementation and operation of data privacy	5	
		Functional	intersects with subset of	Data Privacy Program Data Privacy Program	PRI-01 PRI-01	controls. Mechanisms exist to facilitate the implementation and operation of data privacy	10	
		Functional	intersects with	Restrict Collection To	PRI-04	controls. Mechanisms exist to collect Personal Data (PD) only for the purposes identified in the data privacy notice and includes protections against collecting PD from minors without appropriate parental, or legal guardian, consent.	5	
CC8.1-POF18	Privacy by Design	Functional	intersects with	Authority To Collect, Use, Maintain & Share Personal	PRI-04.1	appropriate parental, or legal guardian, consent. Mechanisms exist to determine and document the legal authority that permits the collection, use, maintenance and sharing of Personal Data (PD), either generally or in	5	
		Functional	intersects with	Data Secure Engineering	SEA-01	support of a specific program or system need. Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and	5	
				Principles Business Continuity		a data privacy practices in the specification, design, development, implementation and modification of systems and services. Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or		
		Functional	intersects with	Management System (BCMS)	BCD-01	Business Continuity & Disaster Recovery (BC/DR) playbooks). Mechanisms exist to implement alternative or compensating controls to satisfy security	5	
		Functional	intersects with	Alternative Security Measures	BCD-07	functions when the primary means of implementing the security function is unavailable or compromised. Mechanisms exist to facilitate the implementation of strategic, operational and tactical	5	
		Functional	intersects with	Risk Management Program Risk Identification	RSK-01 RSK-03	risk management controls. Mechanisms exist to identify and document risks, both internal and external.	5	
		Functional	intersects with	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	
		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	5	
		Functional	intersects with	Threat Catalog	THR-09	hunting, response and recovery activities. Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
		Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls. Mechanisms exist to identify, prioritize and assess suppliers and partners of critical	5	
		Functional	intersects with	Third-Party Criticality Assessments	TPM-02	systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services. Mechanisms exist to evaluate security risks associated with the services and product	5	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Functional	intersects with	Supply Chain Protection Acquisition Strategies,	TPM-03	supply chain. Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique systems, system components or	5	
		Functional	intersects with	Tools & Methods Limit Potential Harm	TPM-03.2	services. Mechanisms exist to utilize security safeguards to limit harm from potential adversaries	5	
		Functional	intersects with	Processes To Address Weaknesses or	TPM-03.3	who identify and target the organization's supply chain. Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	5	
		Functional	intersects with	Deficiencies Third-Party Processing, Storage and Service	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	
		Functional	intersects with	Locations Third-Party Contract	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its	5	
		Functional	intersects with	Requirements Third-Party Personnel Security	TPM-06	systems, processes and data. Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
		Functional	intersects with	Monitoring for Third-Party Information Disclosure	TPM-07	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of organizational information.	5	
		Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity &	5	
		Functional	intersects with	Third-Party Deficiency Remediation	TPM-09	data privacy controls. Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
		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 information, systems and processes that are in scope by the third- party.	5	
		Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
CC9.1-POF1	Considers Mitigation of Risks of Business Disruption	Functional	intersects with	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
		Functional	intersects with	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	5	
		Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
CC9.1-POF2	Considers the Use of Insurance to Mitigate Financial Impact Risks	Functional	intersects with	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
		Functional	intersects with	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	5	
		Functional	subset of	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	10	
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services. Mechanisms exist to facilitate the implementation of third-party management controls.	5	
		Functional	subset of	Third-Party Management Third-Party Risk	TPM-01	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing	10	
		Functional	intersects with	Assessments & Approvals	TPM-04.1	of technology-related services.	5	



FDE#	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (ontional)	Notes (optional)
		Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	and monitoring personnance against under piens. Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	5	
CC9.2-POF1	Establishes Requirements for Vendor and Business Partner Engagements	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
		Functional	intersects with	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
		Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
		Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
		Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	5	
CC9.2-POF2	Identifies Vulnerabilities	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
		Functional	intersects with	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
		Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
		Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	5	
CC9.2-POF3	Assesses Vendor and Business Partner Risks	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
		Functional	intersects with	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
		Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
		Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
CC9.2-POF4	Assigns Responsibility and Accountability for Managing Vendors and Business Partners	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
6521614	reages responsibility and recontinuity for managing ventors and business and incident	Functional	intersects with	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
		Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
CC9.2-POF5	Establishes Communication Protocols for Vendors and Business Partners	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
		Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data. Mechanisms exist to facilitate the implementation of third-party management controls.	5	
		Functional	intersects with	Third-Party Management Third-Party Contract	TPM-01 TPM-05	Mechanisms exist to racinitate the implementation of unit-party management controls. Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its	5	
CC9.2-POF6	Establishes Exception Handling Procedures From Vendors and Business Partners	Functional	intersects with	Requirements Review of Third-Party		systems, processes and data. Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity &	5	
				Services Supply Chain Risk		data privacy controls. Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development. acquisition, maintenance and disposal of systems.		
		Functional	intersects with	Management (SCRM) Plan	RSK-09	system components and services, including documenting selected mitigating actions and monitoring performance against those plans. Mechanisms exist to periodically assess supply chain risks associated with systems,	5	
		Functional	intersects with	Supply Chain Risk Assessment		system components and services. Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC9.2-POF7	Assesses Vendor and Business Partner Performance	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to evaluate security risks associated with the services and product	5	
		Functional	intersects with	Supply Chain Protection	TPM-03	supply chain. Mechanisms exist to perform recurring validation of the Responsible, Accountable,	5	
		Functional	intersects with	Third-Party Scope Review	TPM-05.5	Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity & data privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	
		Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
		Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
		Functional	intersects with	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
CC9.2-POF8	Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments	Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
		Functional	intersects with	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data privacy controls.	5	
		Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
		Functional	intersects with	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
		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 information, systems and processes that are in scope by the third- party.	5	
		Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
		Functional	intersects with	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
CC9.2-POF9	Implements Procedures for Terminating Vendor and Business Partner Relationships	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
		Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
		Functional	intersects with	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data privacy controls.	5	
		Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cy	5	
		Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
		Functional	intersects with	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
CC9.2-POF10	Obtains Confidentiality Commitments From Vendors and Business Partners	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
		Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
		Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compilance with specified statutory, regulatory and contractual obligations for cybescerulty & date privacy controls, including any flow-down requirements to subcontractors.	5	
		Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	5	
CC9.2-POF11	Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
		Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
		Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity & data privacy controls, including any flow-down requirements to subcontractors.	5	
		Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
		Functional	intersects with	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
CC9.2-POF12	Obtains Privacy Commitments From Vendors and Business Partners	Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
		Functional	intersects with	Third-Party Scope Review		Mechanisms exist to perform recurring walidation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity & data privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	
		Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for yeberscurity & data privacy controls, including any flow-down requirements to subcontractors.	5	
		Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data reviews control.	5	
		Functional	intersects with	Threat Intelligence Program	THR-01	data privacy controls. 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	5	
		Functional	intersects with	Indicators of Exposure (IOE)	THR-02	hunting, response and recovery activities. Mechanisms exist to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.	5	
		Functional	intersects with	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
		Functional	intersects with	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected systems, applications and/or services that the organization utilizes.	5	
CC9.2-POF13	Assesses Compliance With Privacy Commitments of Vendors and Business Partners	Functional	intersects with	Monitoring for Third-Party Information Disclosure		Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of organizational information.	5	
		Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
		Functional	intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
		Functional	intersects with	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
		Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
P1.0	Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy	Functional	subset of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data privacy controls.	10	
		Functional	intersects with	Privacy Act Statements	PRI-01.2	Mechanisms exist to provide additional formal notice to individuals from whom the information is being collected that includes collect to Personal Data (PD); *Notice of the authority of organizations to collect Personal Data (PD); *Whether providing Personal Data (PD) is mandatory or optional; *The principal purpose or purposes for which Personal Data (PD) is to be used; *The intended disclosures or routine used of the information *The consequences of not providing all or some portion of the information requested.	5	
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	Functional	intersects with	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to: * Snave that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; * Fanuer that organizational data privacy practices are publicly available through organizational websites or document repositories; * Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(g) regarding data privacy practices; and * Hollman data subjects when changes are made to the privacy notice and the nature of such changes.	5	



FDE II	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; Essures that data privacy notices are clear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meets all legal obligations; Defines 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; Content of the privacy notice is periodically reviewed and updates made as necessary; and Prior versions of the privacy notice are retained in accordance with data retention requirements.	5	
		Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: Alkale data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; - Ensures that data privacy notices are dear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meets all legal obligations; - Defines the scope of PD processing activities, including the geographic locations and dried-party recipients that process the PD within the scope of the data privacy notice; - Content of the privacy notice is periodically reviewed and updates made as necessary; and - Prior versions of the privacy notice are retained in accordance with data retention requirements.	5	
P1.1-P0F1	Communicates to Data Subjects (C)	Functional	intersects with	Purpose Specification		Mechanisms exist to identify and document the purpose(s) for which Personal Data (PD) is collected, used, maintained and shared in its data privacy notices.	5	
P1.1-POF2	Provides Notice to Data Subjects [C]	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: **Aske data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; **Ensures that data privacy notices are clear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meets all legal obligations; **Defines the scope of PD processing activities, including the geographic locations and drief party recipients that procests the Pow thin the scope of the data privacy notice; **Content of the privacy notice is periodically reviewed and updates made as necessary; and **Prior versions of the privacy notice are retained in accordance with data retention requirements. **Mechanisms exists to identify and document the purposety for which Personal Data	5	
		Functional	intersects with	Purpose Specification	PRI-02.1	(PD) is collected, used, maintained and shared in its data privacy notices.	5	
P1.1-POF3	Covers Entities and Activities in Notice (C)	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: Alkale data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; - Sussers that data privacy notices are clear and easy-to-understand, expressing information about Personal Data (PO) processing in plain language that meets all legal obligations; - Defines 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; - Content of the privacy notice is periodically reviewed and updates made as necessary; and - Prior versions of the privacy notice are retained in accordance with data retention requirements.	5	
		Functional	intersects with	Purpose Specification	PRI-02.1	Mechanisms exist to identify and document the purpose(s) for which Personal Data (PD) is collected, used, maintained and shared in its data privacy notices. Mechanisms exist to:	5	
P1.1-POF4	Uses Clear Language and Presents a Current Privacy Notice in a Location Easily Found by Data Subjects [C]	Functional	intersects with	Data Privacy Notice	PRI-02	Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; -Essues that data privacy notices are clear and easy-to-undenstand, expressing information about Personal Data (PD) processing in plain language that meets all legal obligations; -Defines 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; -Content of the privacy notice is periodically reviewed and updates made as necessary; and -Prior versions of the privacy notice are retained in accordance with data retention requirements.	5	
		Functional	intersects with	Purpose Specification	PRI-02.1	Mechanisms exist to identify and document the purpose(s) for which Personal Data (PD) is collected, used, maintained and shared in its data privacy notices.	5	
		Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
P1.1-POF5	Reviews the Privacy Notice [C]	Functional	intersects with	Data Privacy Notice		Mechanism exist to: Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; - Shares that data privacy notices are dear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meets all legal obligations; - Defines the scope of PD processing activities, including the geographic locations and whice-party recipients that process the PD within the scope of the data privacy notice; - Content of the privacy notice is periodically reviewed and updates made as necessary; and - Prior versions of the privacy notice are retained in accordance with data retention requirements.	5	
P1.1-P0F6	Communicates Changes to Notice [C]	Functional	intersects with	Dissemination of Data Privacy Program Information		Mechanism exist to: Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPG) or similar role; Ensure that organizational data privacy practices are publicly available through organizational websites or document repressiontes; Utilize publicly fracing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(g) regarding data privacy practices; and Inform data subjects when changes are made to the privacy notice and the nature of such changes.	5	
P1.1-POF7	Retains Prior Notices [C]	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; Fassures that data privacy notices are clear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meets all legal information about Personal Data (PD) processing in plain language that meets all legal information about Personal Data (PD) processing in plain language that meets all legal information about the stope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; Content of the privacy notice is periodically reviewed and updates made as necessary; and of a processing activities are retained in accordance with data retention requirements.	5	
P2.0	Privacy Criteria Related to Choice and Consent	Functional	subset of	Choice & Consent	PRI-03	Mechanisms exist to authorize the processing of their Personal Data (PD) prior to its collection that: *Uses plain language and provide examples to illustrate the potential data privacy risks of the authorization; and * Provides a means for users to decline the authorization.	10	
P7 1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to authorize the processing of their Personal Data (PD) prior to its collection that: - Uses plan language and provide examples to illustrate the potential data privacy risks of the authorization; and - Provides a means for users to decline the authorization.	5	



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (ontional)	Notes (optional)
12.2	authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the					Mechanisms exist to present authorizations to process Personal Data (PD) in conjunction with the data action, when:	(орцона)	
	collection, use, retention, disclosure, and disposal of personal information is documented.	Functional	intersects with	Just-In-Time Notice & Updated Consent	PRI-03.2	The original circumstances under which an individual gave consent have changed; or A significant amount of time has passed since an individual gave consent.	5	
						Mechanisms exist to authorize the processing of their Personal Data (PD) prior to its		
P2.1-POF1	Communicates to Data Subjects [C]	Functional	intersects with	Choice & Consent	PRI-03	collection that: - Uses plain language and provide examples to illustrate the potential data privacy risks of the authorization; and	5	
						Provides a means for users to decline the authorization.		
						Mechanisms exist to authorize the processing of their Personal Data (PD) prior to its collection that: - Uses plain language and provide examples to illustrate the potential data privacy risks		
P2.1-POF2	Communicates Consequences of Denying or Withdrawing Consent [C]	Functional	intersects with	Choice & Consent	PRI-03	of the authorization; and Provides a means for users to decline the authorization.	5	
						Mechanisms exist to authorize the processing of their Personal Data (PD) prior to its collection that:		
P2.1-POF3	Obtains Implicit or Explicit Consent [C]	Functional	intersects with	Choice & Consent	PRI-03	 Uses plain language and provide examples to illustrate the potential data privacy risks of the authorization; and 	5	
						Provides a means for users to decline the authorization. Mechanisms exist to present authorizations to process Personal Data (PD) in		
P2.1-POF4	Documents and Obtains Consent for New Purposes and Uses [C]	Functional	intersects with	Just-In-Time Notice & Updated Consent	PRI-03.2	conjunction with the data action, when: The original circumstances under which an individual gave consent have changed; or	5	
						 A significant amount of time has passed since an individual gave consent. Mechanisms exist to authorize the processing of their Personal Data (PD) prior to its 		
P2.1-POF5	Obtains Explicit Consent for Sensitive Information [C]	Functional	intersects with	Choice & Consent	PRI-03	collection that: Uses plain language and provide examples to illustrate the potential data privacy risks of the authorization; and	5	
						Provides a means for users to decline the authorization.		
						Mechanisms exist to authorize the processing of their Personal Data (PD) prior to its collection that: - Uses plain language and provide examples to illustrate the potential data privacy risks		
P2.1-POF6	Obtains Consent for Data Transfers [C]	Functional	intersects with	Choice & Consent	PRI-03	To see plant language and provide examples to indistrate the potential data privacy risks of the authorization; and Provides a means for users to decline the authorization.	5	
				Restrict Collection To		Mechanisms exist to collect Personal Data (PD) only for the purposes identified in the data privacy notice and includes protections against collecting PD from minors without		
P3.0	Privacy Criteria Related to Collection	Functional	subset of	Identified Purpose	PRI-04	appropriate parental, or legal guardian, consent.	10	
		Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to collect Personal Data (PD) only for the purposes identified in the data privacy notice and includes protections against collecting PD from minors without appropriate parental, or legal guardian, consent.	5	
P3.1	Personal information is collected consistent with the entity's objectives related to privacy.			Authority To Collect, Use,		Mechanisms exist to determine and document the legal authority that permits the	_	
		Functional	intersects with	Maintain & Share Personal Data	PRI-04.1	collection, use, maintenance and sharing of Personal Data (PD), either generally or in support of a specific program or system need. Mechanisms exist to collect Personal Data (PD) only for the purposes identified in the	5	
P3.1-POF1	Limits the Collection of Personal Information [P][C]	Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	data privacy notice and includes protections against collecting PD from minors without appropriate parental, or legal guardian, consent.	5	
D3 4 D0F3	Called Information by Friend I with Many [DIF]	F	later-rate with	Restrict Collection To	PRI-04	Mechanisms exist to collect Personal Data (PD) only for the purposes identified in the data privacy notice and includes protections against collecting PD from minors without	5	
P3.1-POF2	Collects Information by Fair and Lawful Means [P][C]	Functional	intersects with	Identified Purpose	PRI-04	appropriate parental, or legal guardian, consent. Mechanisms exist to collect Personal Data (PD) only for the purposes identified in the	5	
		Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	mechanisms exist to collect Personal Data (PD) only for the purposes identified in the data privacy notice and includes protections against collecting PD from minors without appropriate parental, or legal guardian, consent.	5	
P3.1-POF3	Collects Information From Reliable Sources [P][C]	Functional	intersects with	Primary Sources	PRI-04.2	Mechanisms exist to ensure information is directly collected from the data subject, whenever possible.	5	
		Tunctional	mersees wer	-	110 04.2	Mechanisms exist to collect Personal Data (PD) only for the purposes identified in the		
P3.1-POF4	Informs Data Subjects When Additional Information Is Acquired [P][C]	Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	data privacy notice and includes protections against collecting PD from minors without appropriate parental, or legal guardian, consent.	5	
		Functional	intersects with	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected or amended.	5	
		Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to authorize the processing of their Personal Data (PD) prior to its collection that: - Uses plain language and provide examples to illustrate the potential data privacy risks	5	
P3.2	For information requiring explicit consent, the entity communicates the need for such consent as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent	Functional	intersects with	Choice & Consent	PRI-US	of the authorization; and Provides a means for users to decline the authorization.	3	
13.2	prior to the collection of the information to meet the entity's objectives related to privacy.			Just-In-Time Notice &		Mechanisms exist to present authorizations to process Personal Data (PD) in conjunction with the data action, when:		
		Functional	intersects with	Updated Consent	PRI-03.2	 The original circumstances under which an individual gave consent have changed; or A significant amount of time has passed since an individual gave consent. 	5	
P3.2-POF1	Informs Data Subjects of Consequences of Failure to Provide Consent [C]	Functional	intersects with	Tailored Consent	PRI-03.1	Mechanisms exist to allow data subjects to modify the use permissions to selected attributes of their Personal Data (PD).	5	
						Mechanisms exist to authorize the processing of their Personal Data (PD) prior to its collection that: - Uses plain language and provide examples to illustrate the potential data privacy risks		
P3.2-POF2	Documents Explicit Consent to Retain Information [C]	Functional	intersects with	Choice & Consent	PRI-03	of the authorization; and Provides a means for users to decline the authorization.	5	
						Mechanisms exist to: • Retain Personal Data (PD), including metadata, for an organization-defined time		
		Functional	subset of	Personal Data Retention &	PRI-05	period to fulfill the purpose(s) identified in the notice or as required by law; • Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of	10	
P4.0	Privacy Criteria Related to Use, Retention, and Disposal			Disposal		storage; and - Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).		
		Functional	subset of	Usage Restrictions of	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	10	
		ranctollal	JUDGET OF	Sensitive Personal Data	03.4	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training	20	
		Functional	intersects with	Internal Use of Personal Data For Testing, Training	PRI-05.1	and research that: • Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and	5	
P4.1	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.			and Research		 Authorizes the use of PD when such information is required for internal testing, training and research. 		
		Functional	intersects with	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	5	
P4.1-POF1	Uses Personal Information for Intended Purposes [P][C]	Functional	intersects with	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	5	
						Mechanisms exist to: • Retain Personal Data (PD), including metadata, for an organization-defined time		
P4.2	The entity retains personal information consistent with the entity's objectives related to privacy.	Functional	intersects with	Personal Data Retention & Disposal	PRI-05	period to fulfill the purpose(s) identified in the notice or as required by law; Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and	5	
				очериза		storage; anno - Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).		
						Mechanisms exist to: • Retain Personal Data (PD), including metadata, for an organization-defined time		
P4.2-POF1	Retains Personal Information [P][C]	Functional	intersects with	Personal Data Retention &	PRI-05	period to fulfill the purpose(s) identified in the notice or as required by law; • Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of	5	
				Disposal		storage; and • Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).		
P4.2-P0F2	Protects Personal Information [P][C]	Functional	intersects with	Security of Personal Data	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of	5	
. +.2-rOF2		Functional	intersects with	Sanitization of Personal	DCH-09.3	are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD. Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5	
		Functional	intersects with	Data (PD) Information Disposal		Mechanisms exist to securely dispose of, destroy or erase information.	5	



### 18	FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
### 18							Mechanisms exist to:	(optional)	
Hand in the second problem of the p	P4.3	The entity securely disposes of personal information to meet the entity's objectives related to privacy.	Functional	intersects with		PRI-05	period to fulfill the purpose(s) identified in the notice or as required by law; • Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of	5	
Heater the section of					Disposai		Use organization-defined techniques or methods to ensure secure deletion or		
Heat Properties of the Control of Service (1997) (Functional	intersects with		PRI-06.4		5	
Hand the second	P4.3-POF1	Captures, Identifies, and Flags Requests for Deletion [P][C]					practices.		
Handle Manufacture for the control of the control			Functional	intersects with		PRI-06.5	Mechanisms exist to securely dispose of, destroy or repurpose system components	5	
Part			Functional	intersects with	Destruction or Re-Use of	AST-09	using organization-defined techniques and methods to prevent information being recovered from these components.		
### 1865 ##					· ·		formal procedures.		
### 1800년 ###	P4.3-POF2	Disposes of, Destroys, and Redacts Personal Information [P][C]	Functional	intersects with	Information Disposal	DCH-21	Mechanisms exist to:	,	
Hand to the second PD seco			Sunational		Personal Data Retention &	DDI OF	period to fulfill the purpose(s) identified in the notice or as required by law;	-	
## 1985			Punctional	intersects with	Disposal	FRI-03	Use organization-defined techniques or methods to ensure secure deletion or	,	
### 1870							Mechanisms exist to securely dispose of, destroy or repurpose system components		
Part					Equipment		recovered from these components.		
Part					,		formal procedures.		
Part	P4.3-POF3	Destroys Personal Information [P][C]							
March Marc			Functional	intersects with		PRI-05	period to fulfill the purpose(s) identified in the notice or as required by law; • Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of	5	
Mathematical Continues Mathematical Contin					Disposal		Use organization-defined techniques or methods to ensure secure deletion or		
Part	P5.0	Privacy Criteria Related to Access	Functional	subset of	Data Subject Access	PRI-06	Mechanisms exist to provide data subjects the ability to access their Personal Data (PD)	10	
Proof Proo							Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is		
Part			Functional	intersects with		DCH-22.1	identified.	5	
	P5.1	for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason	Functional	intersects with	Data Subject Access	PRI-06		5	
Section Sect		for such denial, as required, to meet the entity's objectives related to privacy.			Unio Franklandi				
1			Functional	intersects with		PRI-06.4	practices.	5	
1							maintained in organizational systems of records.		
							maintained in organizational systems of records.		
1	P5.1-P0F3	Permits Data subjects Access to Their Personal Information [P][C]			User Feedback		Mechanisms exist to implement a process for receiving and responding to complaints,		
	P5.1-POF4	Provides Understandable Personal Information Within Reasonable Time [P][C]					practices.		
Manual Desiration Manu			Functional	intersects with	Disclosure Requests	PRI-07.4	Mechanisms exist to implement a process for receiving and responding to complaints.	5	
Part	P5.1-POF5	Informs Data Subjects If Access is Denied [P][C]	Functional	intersects with	User Feedback Management	PRI-06.4	concerns or questions from data subjects about the organizational data privacy practices.	5	
Part			Functional	intersects with		DCH-22.1	inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-	5	
Pacifical and patients Pacifical and patie							Mechanisms exist to establish and implement a process for:		
Has ester connect, among, or agreed personal information provided by active adjustment to an information and provided by activation of the client of an information and provided by activation of the client of an information and provided by activation of the client of an information and provided by activation of the client of an information and provided by activation of the client of an information and provided by activation of the client of an information and provided by activation (activation and provided by activation and provided by activation (activation and provided by activation and provided by			Functional	intersects with		PRI-06.1	corrected or amended; and	5	
P3.2 Processory Contents among or departed programme processory forming to proceed by reflective or information processory and reported by a formation or information and processory or agreement or processor or account programme and are processory or account processor or account or processor or account processor or accou					Notice of Correction or				
Functional interacts with Punctional Interac	P5.2	and communicates such information to third parties, as committed or required, to meet the entity's objectives	Functional	intersects with		PRI-06.2		5	
P3.29072 Provided Pro		such denial to meet the entity's objectives related to privacy.	Functional	intersects with	Appeal Adverse Decision	PRI-06.3		5	
Pactional elements with functional elements with functional elements with functional elements with functional elements of control processes to descript an execution and project or processes of the control processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method and processes to descript and record the method and processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional processes to descript and record the method under which functional pro					Hear Foodback				
Post closed Post Colon Interacts with Updating Promoted Data Post P			Functional	intersects with	Management	PRI-06.4	practices.	5	
Functional intersects with Parameters with Par			Functional	intersects with		PRI-12	Mechanisms exist to develop processes to identify and record the method under which Personal Data (PD) is updated and the frequency that such updates occur.	5	
PS.3 POFT Regionds to Data Controller Requests (P) Regions to Data Controller Regions to Data Subjects of Data Subjects (P) Re			Europeten 1	into		DP: 0" .		-	
Functional Intersects with Processing Change PS-2-PG/2 Communicates Denial of Access Requests (P[C]	P5.2-POF1	Responds to Data Controller Requests [P]	runctional			PRI-Ub.4	practices.	3	
PS.2-POF2 Communicates Denial of Access Requests [P][C] Functional intersects with Punctional intersects with Processing Change PS.2-POF3 Permits Data Subjects to Update or Correct Personal Information [P][C] Functional intersects with Punctional intersects with Processing Change PS.2-POF4 PS.2-POF6 Processing Change PS.2-POF6 PS.2-POF6 Processing Change PS.2-POF6			Functional	intersects with		PRI-07.4		5	
PS.2-POF2 Communicates Denial of Access Requests [P][C] Functional intersects with Processing Change Functional i			Functional	intersects with		PRI-06.1	 Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and 	5	
P3.2-POF2 Communicates Denial of Access Requests [P][C] Functional intersects with Processing Change Functional intersects with Processing Change Functional intersects with Processing Change Functional intersects with Personal Data [P]] is updated and the frequency that such updates occur. 5 P8-12 P8.12 P8.12 P8.12 P8.12 P8.12 P8.13 Permits Data Subjects to Update or Correct Personal Information [P][C] P8.2-POF3 Permits Data Subjects to Update or Correct Personal Information [P][C] P8.2-POF3 Permits Data Subjects to Update or Correct Personal Information [P][C] P8.2-POF4 Prunctional intersects with Processing Change P8.10									
PR-12 PR-1	P5.2-POF2	Communicates Denial of Access Requests [P][C]	Functional	intersects with		PRI-06.2		5	
Functional intersects with Participated inter			Power 1		Updating Personal Data	pp:			
PS.2-PDF3 Permits Data Subjects to Update or Correct Personal Information [P][C] Functional intersects with Principles of PRI-06.2 Corrected or amended. PS.2-PDF4 Communicates Denial of Correction Requests [P][C] Functional intersects with Principles of Privacy Citeria Related to Disclosure Requests [P][C] Functional intersects with Principles of Privacy Citeria Related to Disclosure Requests (P)[C] Functional intersects with Principles of Privacy Citeria Related to Disclosure Requests (P)[C] Privacy Citeria Related to Disclosure and Notification Privacy Citeria Related to Disclosure Requests (P)[C] Privacy Citeria Related to Disclosure Requests (P)[C] Privacy Citeria Related to Disclosure Requests (P)[C] Privacy Citeria Related to Disclosure and Notification Privacy Citeria Related to Disclosure and Notification Privacy Citeria Related to Disclosure Repulsional Association Privacy Citeria Related (P)[C] Privacy Citeria Relat			Functional	intersects with		PKI-12		5	
P5.2-PDF3 Permits Data Subjects to Update or Correct Personal Information [P][C] Functional intersects with Management P5.2-PDF4 Communicates Denial of Correction Requests [P][C] Functional intersects with Reject Unauthorized Denial of Correction Requests [P][C] Functional intersects with Reject Unauthorized Denial of Correction Requests [P][C] Functional intersects with Reject Unauthorized Denial of Correction Requests [P][C] Functional intersects with Reject Unauthorized Denial of Correction Requests [P][C] Functional intersects with Reject Unauthorized Denial of Correction Requests [P][C] Functional intersects with Reject Unauthorized Denial of Correction Requests [P][C] Functional intersects with Reject Unauthorized Denial of Correction Requests [P][C] Functional intersects with Reject Unauthorized Denial of Correction Requests [P][C] Functional intersects with Reject Unauthorized Denial of Correction Requests [P][C] Functional intersects with Reject Unauthorized Denial of Correction Requests [P][C] Functional intersects with Reject Unauthorized Denial of Correction Requests [P][C] Functional intersects with Reject Unauthorized Denial of Correction Requests [P][C] Functional intersects with Reject Unauthorized Denial of Correction Requests [P][C] Functional intersects with Reject Unauthorized Denial of Correction Requests [P][C] Functional intersects with Reject Denial Den			Functional	intersects with		PRI-06.2		5	
Functional intersects with Management PR-0.4 practices. 5 Functional intersects with PR-0.7 practices. 5 Functional intersects with PR-0.7 practices. 5 Functional intersects with Reject Unauthorized Disclosure Requests PR-0.7 practices. 5 Fig. 27-PF4 Communicates Denial of Correction Requests [P][C] Functional intersects with Intersects with Rehalance with PR-0.5 practices. 5 Fig. 27-PF4 Communicates Denial of Correction Requests [P][C] Functional intersects with Intersects with Principles of Contents of Disclosure and Notification Practices of PR-0.5 practices. 5 Fig. 27-PF4 Communicates Denial of Correction Requests [P][C] Functional Subjects and such Intersects with In									
P3.2-POF4 Communicates Denial of Correction Requests [P][C] Functional Intersects with Disclosure Requests with Disclosure Requests PRI-O3.4 P5.2-POF4 Communicates Denial of Correction Requests [P][C] Functional Intersects with Prince Parties P6.0 Privacy Criteria Related to Disclosure and Notification Privacy Priv	P5.2-POF3	Permits Data Subjects to Update or Correct Personal Information [P][C]	Functional	intersects with		PRI-06.4	practices.	5	
P5.2-PDF4 Communicates Denial of Correction Requests [P][C] Functional intersects with Information Sharing With Tourised and the Consent is obtained prior to disclosure to meet the entity's objectives related to privacy. P6.1 The entity discloses personal information to third parties with the explicit consent of data subjects and such Consent is obtained prior to disclosure to meet the entity's objectives related to privacy. P8.0.4 Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy of sensitive / regulated data to authorized purities with a need to know. P8.0.5 Mechanisms exist to bestore the disclosure of sensitive / regulated data to authorized purities with a need to know. P8.0.5 Mechanisms exist to disclosure or sensitive / regulated data to authorized purities with a need to know. P8.0.7 Mechanisms exist to disclosure end with the implicit or explicit consent of the data subjects and such information Sharing With Third Parties. P8.0.7 Mechanisms exist to disclosure end with the implicit or explicit consent of the data subjects and such information Sharing With Third Parties. P8.0.7 Mechanisms exist to disclosure end with the implicit or explicit consent of the data subjects and with the implicit or explicit consent of the data subjects. P8.0.7 Mechanisms exist to disclosure end with the implicit or explicit consent of the data subjects about the organizational data privacy or disclosure from data subjects about the organizational data privacy or disclosure from data subjects about the organizational data privacy or disclosure from data subjects about the organizational data privacy or disclosure from data subjects about the organizational data privacy or disclosure from data subjects about the organizational data privacy or disclosure from data subjects about the organizational data privacy or descent with the implicit or explicit consent of the data subjec			Functional	intersects with		PRI-07.4	Mechanisms exist to reject unauthorized disclosure requests.	5	
P6.0 Privacy Criteria Related to Disclosure and Notification P6.1 The entity discloses personal information to their dupraties with the explicit consent of data subjects and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy. P6.1 The entity discloses personal information to their dupraties with the explicit consent of data subjects and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy. P6.1 The entity discloses personal information to their dupraties only for the purposes of the data privacy notice and with the implicit or explicit consent of the data privacy notice and with the implicit or explicit consent of the data is a subject. South is object to send to the object of the purpose of the data privacy notice and with the implicit or explicit consent of the data is a subject. South is object to send the constitution of the purpose of the data privacy notice and with the implicit or explicit consent of the data is a subject. South is object. The discourse of the data is a subject and on the object or explicit consent of the data is a subject and on the object. The discourse of the data is a subject and the object or explicit consent of the data is a subject and on the object or explicit consent of the data is a subject and on the object. The object or explicit consent of the data is a subject and the object. The object or explicit consent of the data is a subject and on the object. The object or explicit consent of the data is a subject and the object. The object or explicit consent of the data is a subject and the object or explicit consent of the data is a subject and the object. The object or explicit consent of the data is a subject and the object or explicit consent of the data is a subject and the object or explicit consent of the data is a subject and the object or explicit consent of the data is a subject and the object or explicit consent of the data is a subject and the object or explicit consent of the dat	<u> </u>				-				
P6.1 The entity disclose personal information to this parties with the explicit consent of data subjects and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy. Functional Fun					Management		practices.		
P6.1 If the clinity valuebase per some information of white purposes and summation of the data privacy notice and with the implicit or explicit consent of the data of the dat		·					parties with a need to know. Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes		
Functional intersects with intersects with intersects with Starting with intersects with Starting with intersects with Starting with intersects with Starting with Startin	P6.1		Functional	intersects with	Third Parties	PRI-07	subject.	5	
			Functional	intersects with		PRI-07	identified in the data privacy notice and with the implicit or explicit consent of the data	5	



FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
P6.1-P0F1	Communicates Privacy Policies to Third Parties [P][C]	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	
		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	
P6.1-P0F2	Discloses Personal Information Only When Appropriate [P][C]	Functional	intersects with	Limiting Personal Data Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	5	
		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	
P6.1-POF3	Discloses Personal Information Only to Appropriate Third Parties [P][C]	Functional	intersects with	Limiting Personal Data Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	5	
P6.1-P0F4	Discloses information to Third Parties for New Purposes and Uses [P][C]	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	
F0.1-F0F4		Functional	intersects with	Limiting Personal Data Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained. Mechanisms exist to develop and maintain an accounting of disclosures of Personal	5	
P6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.	Functional	intersects with	Accounting of Disclosures	PRI-14.1	Data (PD) held by the organization and make the accounting of disclosures available to the person named in the record, upon request. Mechanisms exist to develop and maintain an accounting of disclosures of Personal	5	
P6.2-POF1	Creates and Retains Record of Authorized Disclosures [P][C]	Functional	subset of	Accounting of Disclosures	PRI-14.1	Data (PD) held by the organization and make the accounting of disclosures available to the person named in the record, upon request. Mechanisms exist to address data breaches, or other incidents involving the	10	
		Functional	intersects with	Data Breach	IRO-04.1	unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations. Mechanisms exist to timely-report incidents to applicable:	5	
P6.3	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Internal stakeholders; Affected clients & third-parties; and Regulatory authorities.	5	
		Functional	intersects with	Information Spillage Response	IRO-12	Mechanisms exist to respond to sensitive information spills. Mechanisms exist to develop and maintain an accounting of disclosures of Personal	5	
		Functional	intersects with	Accounting of Disclosures	PRI-14.1	Data (PD) held by the organization and make the accounting of disclosures available to the person named in the record, upon request. Mechanisms exist to develop and maintain an accounting of disclosures of Personal	5	
P6.3-POF1	Creates and Retains Record of Detected or Reported Unauthorized Disclosures [P] [C]	Functional	subset of	Accounting of Disclosures	PRI-14.1	Data (PD) held by the organization and make the accounting of disclosures available to the person named in the record, upon request. Mechanisms exist to include data privacy requirements in contracts and other	10	
P6.4	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	Functional	subset of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
P6.4-POF1	Evaluates Third-Party Compliance With Privacy Commitments [P][C]	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	
10.41012	Community (Tip)	Functional	intersects with	Limiting Personal Data Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	5	
		Functional	intersects with	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5	
P6.4-POF2	Remediates Misuse of Personal Information by a Third Party [P][C]	Functional	intersects with	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data privacy controls.	5	
		Functional	intersects with	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
		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	
P6.4-POF3	Obtains Commitments to Report Unauthorized Disclosures [P][C]	Functional	intersects with	Third-Party Contract	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its	5	
		Functional	intersects with	Requirements Contract Flow-Down	TPM-05.2	systems, processes and data. Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
P6.5	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident- response procedures to meet the entity's objectives related to privacy.	Functional	intersects with	Requirements Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	
	responde procedures to meet the entity a objective reduced to privacy.	Functional	intersects with	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5	
P6.5-POF1	Remediates Misuse of Personal Information by a Third Party [P][C]	Functional	intersects with	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data privacy controls.	5	
		Functional	intersects with	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
		Functional	intersects with	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5	
P6.5-POF2	Reports Actual or Suspected Unauthorized Disclosures [P][C]	Functional	intersects with	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data privacy controls.	5	
		Functional	intersects with	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
		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,	5	
P6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.	Functional	intersects with	Third-Party Incident Response & Recovery	TPM-11	regulations and contractual obligations. Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	
		Functional	intersects with	Capabilities Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5	
P6.6-POF1	Identifies Reporting Requirements [P][C]	Functional	intersects with	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data privacy controls.	5	
		Functional	intersects with	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
P6.6-POF2	Provides Notice of Breaches and Incidents [P][C]	Functional	equal	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,	10	
		Functional	intersects with	Data Breach	IRO-04.1	regulations and contractual obligations. 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.	5	
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	regulations and contractual obligations. Mechanisms exist to timely-report incidents to applicable: Internal stakeholders; Affected clients & third-parties; and	5	
		Functional	intersects with	Purpose Specification	PRI-02.1	Regulatory authorities. Mechanisms exist to identify and document the purpose(s) for which Personal Data (PD) is collected, used, maintained and shared in its data privacy notices.	5	
		Functional	intersects with	Authority To Collect, Use, Maintain & Share Personal Data	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the collection, use, maintenance and sharing of Personal Data (PD), either generally or in content of a possible pergraph of purpose of purpose.	5	
P6.7-P0F1	Responds to Data Controller Requests [P]	Functional	intersects with	Business Process Definition	PRM-06	support of a specific program or system need. Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: The resulting risk to organizational operations, assets, individuals and other organizations; and Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
		Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
P6.7-POF2	Identifies Types of Personal Information and Handling Process [P][C]	Functional	intersects with	Data Portability	PRI-06.6	purscues. Mechanisms exist to export Personal Data (PD) in a structured, commonly used and machine-readable format that allows the data subject to transmit the data to another controller without hindrance. Mechanisms exist to digitally export Personal Data (PD) in a secure manner upon	5	
		Functional	intersects with	Personal Data Exportability	PRI-06.7	request by the data subject.	5	



FDE#	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
		Functional	intersects with	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects such that the material is readily accessible and written in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
P6.7-POF3	Captures, identifies, and Communicates Requests for Information [P][C]	Functional	intersects with	Data Controller Communications	PRI-18	Mechanisms exist to receive and respond to contractual obligations from data controllers that includes: - Obta subject requests; - Updates/corrections to Personal Data (PD); - Updates/corrections to Desonal Data (PD); - Obliciosiums: of PD: and - Accounting for PD that is stored, processed and/or transmitted on behalf of the data controller.	5	
P7.0	Privacy Criteria Related to Quality	Functional	intersects with	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	5	
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	Functional	intersects with	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information	5	
P7.1-P0F1	Ensures Accuracy and Completeness of Personal Information [P][C]	Functional	intersects with	Data Quality Management	PRI-10	lifecycle. Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	5	
P7.1-POF2	Ensures Relevance of Personal Information [P][C]	Functional	intersects with	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	5	
P8.0	Privacy Criteria Related to Monitoring and Enforcement	Functional	intersects with	Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct cybersecurity & data privacy testing, training and monitoring activities	5	
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
P8.1-POF1	Communicates to Data Subjects or Data Controllers [P][C]	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
P8.1-POF2	Addresses Inquiries, Complaints, and Disputes [P][C]	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
P8.1-POF3	Documents and Communicates Dispute Resolution and Recourse [P][C]	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
P8.1-POF4	Documents and Reports Compliance Review Results [P][C]	Functional	intersects with	Data Privacy Records & Reporting	PRI-14	Mechanisms exist to maintain data privacy-related records and develop, disseminate and update reports to internal senior management, as well as external oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory data privacy program mandates.	5	
P8.1-POF5	Documents and Reports Instances of Noncompliance [P][C]	Functional	intersects with	Data Privacy Records & Reporting	PRI-14	Mechanisms exist to maintain data privacy-related records and develop, disseminate and update reports to internal senior management, as well as external oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory data privacy program mandates.	5	
P8.1-POF6	Performs Ongoing Monitoring [P][C]	Functional	intersects with	Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct cybersecurity & data privacy testing, training and monitoring activities	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate palaming, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
PI1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: - The resulting risk to organizational operations, assets, individuals and other organizations, and - information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
		Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
		Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
		Functional	intersects with	Criticality Analysis	TDA-06.1	Mechanisms exist to require the developer of the system, system component or service to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	
		Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
PI1.1-POF1	Identifies Functional and Monfunctional Requirements and Information Specifications	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for ophersecurity & data privacy that determines: *The resulting risk to organizational peratotion, assets, individuals and other organizations, and *Information protection needs arising from the defined business processes and revises the processes as necessary, until an archievable set of protection needs is obtained.	5	
		Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to update products, including systems, software and services, to improve functionality and correct	5	
		Functional	intersects with	Minimum Viable Product (MVP) Security Requirements	TDA-02	security deficiencies. Mechanisms exist to ensure risk-based technical and functional specifications are established to define a Minimum Viable Product (MVP).	5	
		Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components to services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
PI1.1-POF2	Defines Data Necessary to Support a Product or Service	Functional	intersects with	Product Management	TDA-01.1	Mechanism exist to design and implement product management processes to update products, including systems, software and services, to improve functionality and correct security deficiencies.	5	



FDE #	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF #	Secure Controls Framework (SCF)	Strength of Relationship	Notes (optional)
		Rationale	Relationship			Control Description Mechanisms exist to ensure risk-based technical and functional specifications are	(optional)	,
		Functional	intersects with	Minimum Viable Product (MVP) Security Requirements	TDA-02	established to define a Minimum Viable Product (MVP).	5	
		Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition		Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC). Mechanisms exist to design and implement product management processes to update	5	
PI1.1-POF3	Defines Information Necessary to Support the Use of a Good or Product	Functional	intersects with	Product Management		products, including systems, software and services, to improve functionality and correct security deficiencies.	5	
		Functional	intersects with	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to ensure risk-based technical and functional specifications are established to define a Minimum Viable Product (MVP).	5	
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives	Functional	subset of	Technology Development & Acquisition Secure Coding	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs. Mechanisms exist to develop applications based on secure coding principles.	10	
		Functional	intersects with		TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
PI1.2-POF1	Defines Characteristics of Processing Inputs	Functional	intersects with	Secure Coding Input Data Validation	TDA-06	Mechanisms exist to check the validity of information inputs.	5	
		Functional	intersects with	Secure Coding	TDA-18	Mechanisms exist to develop applications based on secure coding principles.	5	
PI1.2-POF2	Evaluates Processing Inputs	Functional	intersects with	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
		Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
PI1.2-POF3	Creates and Maintains Records of System Inputs	Functional	intersects with	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
PI1.3	The entity implements policies and procedures over system processing to result in products, services,	Functional	subset of	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.	10	
		Functional	equal	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	10	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
PI1.3-POF1	Defines Processing Specifications	Functional	intersects with	Business Process Definition		Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: The resulting risk to organizational operations, assets, individuals and other organizations, and "of the organizations and "of the organizations and "of the organizations protection needs arising from the defined business processes and revises the processes as necessary, until an archievable set of protection needs is obtained.	5	
		Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanism exist to define supporting business processes and implement appropriate powernance and sortion entangement on neuroa appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
PI1.3-POF2	Defines Processing Activities	Functional	intersects with	Business Process Definition		Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: - The resulting risk to organizational operations, assets, individuals and other organizations; and - Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
		Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, editivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
PI1.3-POF3	Detects and Corrects Processing or Production Activity Errors	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for ophersecurity & data privacy that determines: The resulting risk to organizational operations, assets, individuals and other organizations, and "office and other organizations," and "office and other organizations protection needs arising from the defined business processes and revises the processes are necessary, until an achievable set of protection needs is obtained.	5	
		Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanism exist to define supporting business processes and implement appropriate governance and severe management to incurse appropriate planning, deliven and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
P11.3-POF4	Records System Processing Activities	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: - The resulting risk to organizational operations, assets, individuals and other organizations, and - information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
		Functional	intersects with	Secure Coding	1DA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting businesy processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or exustomers based on industry-recognized standards to achieve the specific goals of the process area.	5	
PI1.3-POF5	Processes Inputs	Functional	intersects with	Business Process Definition		Mechanisms exist to define business processes with consideration for optersecurity & data privacy that determines: - The resulting risk to organizational operations, assets, individuals and other organizations, and - Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
		Functional	intersects with	Secure Coding	IDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
		Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: 1 stabilish what type of event occurred; 1 when (date and time) the event occurred; 1 when (date and time) the event occurred; 1 where the event occurred; 1 The source of the event; 1 The outcome (success or failure) of the event; and	5	
PI1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accurriance with snecifications to meet the entity's objectives			<u> </u>		The identity of any user/subject associated with the event.		



PII.4-POF1 Prot	the december of the second sec	Functional	intersects with	Protection of Event Logs		Mechanisms exist to protect event logs and audit tools from unauthorized access,	5	
PI1.4-POF1 Prot		Functional			MON-08	modification and deletion.	-	
P11.4-POF1 Prot			intersects with	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	5	
PII.4-POF1 Prot		Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
PII.4-POF1 Prot		Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
PI1.4-POF1 Prot		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
	otects Output	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: "The resulting risk to organizational operations, assets, individuals and other organizations; and "Information protection needs arising from the defined business processes and revises "Information protection needs arising from the defined business processes and revises "Information protection needs arising from the defined business processes and revises "Information protection needs arising from the defined business processes and revises "Information protection needs arising from the defined business processes and revises "Information protection needs arising from the defined business processes and revises "Information protection needs arising from the defined business processes and revises "Information protection needs arising from the defined business processes and revises "Information protection needs arising from the defined business processes and revises "Information protection needs arising from the defined business processes and revises "Information protection needs arising from the defined business processes and revises "Information protection needs arising from the defined business processes and revises "Information protection needs arising from the defined business processes and "Information protection needs arising from the defined business processes are "Information protection needs arising from the defined business processes are "Information protection needs arising from the "Information protecti	5	
		Functional	intersects with	Secure Coding	TDA-06	the processes as necessary, until an achievable set of protection needs is obtained. Mechanisms exist to develop applications based on secure coding principles.	5	
		Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, worlforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
PI1.4-POF2 Distri	tributes Output Only to Intended Parties	Functional	intersects with	Business Process Definition		Mechanisms exist to define business processes with consideration for ophersecurity & data privacy that determines: * The resulting risk to organizational operations, assets, individuals and other organizations; and "sindomation protection needs arising from the defined business processes and revises the processes as necessary, until an archievable set of protection needs is obtained.	5	
		Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
		Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanism exist to define supporting business processes and implement appropriate governance and service management or ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or sustomers based on industry-recognized standards to achieve the specific goals of the process area.	5	
PI1.4-POF3 Distri	tributes Output Completely and Accurately	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: * The resulting risk to organizational operations, assets, individuals and other organizations; and in the control of the contro	5	
						the processes as necessary, until an achievable set of protection needs is obtained. Mechanisms exist to develop applications based on secure coding principles.		
		Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles. Mechanisms exist to facilitate the implementation of data protection controls.	5	
		Functional	intersects with	Data Protection Service Delivery (Business Process Support)	DCH-01 OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or_customers based on industry-recognized standards to achieve the	5	
PI1.4-POF4 Crea	eates and Maintains Records of System Output Activities	Functional	intersects with	Business Process Definition	PRM-06	specific goals of the process area. Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: * The resulting risk to organizational operations, assets, individuals and other organizations; and "information protection needs arising from the defined business processes and revises the processes are ancessany, until an archievable set of protection needs is obtained.	5	
		Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
		Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
The	e entity implements policies and procedures to store inputs, items in processing, and outputs completely,	Functional	intersects with	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
	curately, and timely in accordance with system specifications to meet the entity's objectives.	Functional	intersects with	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
		Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
		Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanism exist to define supporting business processes and implement appropriate governance and service management or neuror appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or sustomers based on industry-recognized standards to achieve the specific goals of the process area.	5	
PI1.5-POF1 Prot	stects Stored Items	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: * The resulting risk to organizational operations, assets, individuals and other organizations; and * Information protection needs arising from the defined business processes and revises the processes are necessary, until an archievable set of protection needs is obtained.	5	
		Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
		Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
PI1.5-POF2 Arch	hives and Protects System Records	Functional	intersects with	Business Process Definition	PRM-06	Mechanism exist to define business processes with onsideration for cybenecurity & data privacy that determines: * The resulting risk to organizational operations, assets, individuals and other organizations; and in the organizations; and in the organizations; and in the organizations are also as a fine organization and a single from the defined business processes and revises the processes are necessary, until an achievable set of protection needs is obtained.	5	
		Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
		Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, edielery and compared to the process of the workforce, adult or ustomers based on industry-recognized standards to achieve the specific goals of the process area.	5	
PI1.5-POF3 Ston	Stores Data Completely and Accurately	Functional	intersects with	Business Process Definition		Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: - The resulting risk to organizational operations, assets, individuals and other organizations; and - information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
		Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
		Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management on ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	



Version 2024.2 5/22/2024

FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
PI1.5-POF4	Creates and Maintains Records of System Storage Activities	Functional	intersects with	Business Process Definition		Mechanisms exist to define business processes with consideration for cybersecurity & data princy that determines: The resulting risk to organizational operations, assets, individuals and other organizations; and Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
		Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	

