NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework; (SCF) version 2025.3
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document URL: https://www.aicpo.org/interestiness/firc/assuranceady/soyservices/aicpasoc2report.html https://www.aicpo.org/interestiness/firc/assuranceady/soyservices/aicpasoc2report.html https://securecontrolsframework.com/content/strm/scf-strm-general-aicpa-tos-2017.pdf

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
A1.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	
A1.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.1-POF1	Measures Current Usage	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
A1.1-POF1	Measures Current Usage	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Performance Monitoring	CAP-04	capacity requirements. Automated mechanisms exist to centrally-monitor and slert on the operating state and health status of critical Technology Assets, Applications and/or Services (TAAS).	10	
A1.1-POF2	Forecasts Capacity	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	10	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	casacity requirements. Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) talkyooksis.	10	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Backups	BCD-11	Mechanisms exists to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Transaction Recovery	BCD-12.1	Mechanisms exist to utilize specialized backup mechanisms that will allow transaction recovery for transaction-based Technology Assets, Applications and/or Services (TAAS) in accordance with Recovery Point Objectives (RPOs).	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Failover Capability	BCD-12.2	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical Technology Assets, Applications, Services and/or Data (TAASD)	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical & Environmental Protections	PES-01	I late it in a still the control of physical and environmental protection controls.	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Automatic Voltage Controls	PES-07.1	Facility security mechanisms exist to utilize automatic voltage controls for critical system components.	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Emergency Shutoff	PES-07.2	Facility security mechanisms exist to shut off power in emergency situations by: (I) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and (2) Protecting emergency power shutoff capability from unauthorized activation.	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Emergency Lighting	PES-07.4	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	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Water Damage Protection	PES-07.5	emergency 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	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Fire Protection	PES-08	properly and 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	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Fire Detection Devices	PES-08.1	energy source. Facility security mechanisms exist to utilize and maintain fire detection devices/systems that activate automatically and notify organizational personnel and	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Fire Suppression Devices	PES-08.2	emergency 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	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Temperature & Humidity	PES-09	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Controls Monitoring with Alarms /	PES-09.1	Facility security mechanisms exist to trigger an atarm or notification of temperature and humidity changes that be potentially harmful to personnel or equipment.	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Notifications 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	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Alternate Work Site	PES-10	points such as derivery and loading areas and other points to avoid unauthorized access. Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Equipment Siting &	PES-11	Physical security mechanisms exist to locate system components within the facility	5	
					Protection Information Leakage Due		to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. Facility security mechanisms exist to protect the system from information leakage		
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	To Electromagnetic Signals Emanations Electromagnetic Pulse	PES-13	due to electromagnetic signals emanations. Physical security mechanisms exist to employ safeguards against Electromagnetic	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(EMP) Protection	PES-15	Pulse (EMP) damage for systems and system components. Mechanisms exist to identify and document risks, both internal and external.	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Identification	RSK-03		5	



Secure Controls Framework (SCF)

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets,	5	
A1.2-POF1	Identifies Environmental Threats	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Apolications. Services and/or Data (TAASD). Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery	5	
A1.2-POF1	Identifies Environmental Threats	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical & Environmental Protections	PES-01	BC/DRI olavbooks). Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
A1.2-POF1	Identifies Environmental Threats	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
A1.2-POF1	Identifies Environmental Threats	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	10	
A1.2-POF2	Designs Detection Measures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) olswbooks).	5	
A1.2-POF2	Designs Detection Measures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
A1.2-POF2	Designs Detection Measures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
A1.2-POF2	Designs Detection Measures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Notifications Business Continuity	PES-09.1	and humidity changes that be potentially harmful to personnel or equipment. Mechanisms exist to facilitate the implementation of contingency planning controls	5	
A1.2-POF3		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management System (BCMS)	BCD-01	to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) otavbooks). Mechanisms exist to facilitate the operation of physical and environmental	5	
A1.2-POF3	Maintains Environmental Protection Mechanisms	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Physical & Environmental Protections	PES-01	protection controls. Mechanisms exist to facilitate the implementation of contingency planning controls	10	
A1.2-POF4	Implements Alerts to Analyze Anomalies	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
A1.2-POF4	Implements Alerts to Analyze Anomalies	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
A1.2-POF4	Implements Alerts to Analyze Anomalies	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Temperature & Humidity Controls	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	5	
A1.2-POF4	Implements Alerts to Analyze Anomalies	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Monitoring with Alarms / Notifications	PES-09.1	and humidity changes that be potentially harmful to personnel or equipment.	5	
A1.2-POF5	Responds to Environmental Threat Events	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
A1.2-POF5	Responds to Environmental Threat Events	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
A1.2-POF5	Responds to Environmental Threat Events	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2-POF5	Responds to Environmental Threat Events Communicates and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) ptsybooks).	10	
A1.2-POF6	Communicates and Reviews Detected Environmental Threat Events	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
A1.2-POF7 A1.2-POF7	Determines Data Determines Data Requiring Backup	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	subset of intersects with	Data Protection Sensitive / Regulated Data Protection	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 5	
A1.2-POF7	Determines Data Requiring Backup	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives	5	
A1.2-POF7	Determines Data Requiring Backup	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical & Environmental Protections	PES-01	(RPOs). Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
A1.2-POF8	Performs Data Backup	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
A1.2-POF9	Addresses Offsite Storage	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Alternate Storage Site	BCD-08	IMPUSI. 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	
A1.2-POF9	Addresses Offsite Storage	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2-POF9	Addresses Offsite Storage	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Transfer to Alternate Storage Site	BCD-11.6	Mechanisms exist to transfer backup data to the alternate storage site at a rate that is	5	
A1.2-POF9	Addresses Offsite Storage	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery	10	
A1.2-POF10	Implements Alternate Processing Infrastructure	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Alternate Processing Site	BCD-09	IRC/DRI olavbooks). Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	10	
A1.2-POF11	Considers Data Recoverability	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BSC/DR) olaybooks).	5	
A1.2-P0F11	Considers Data Recoverability	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Framing	RSK-01.1	Indication interesting the control of the control o	5	
A1.2-POF11	Considers Data Recoverability	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
A1.2-POF11	Considers Data Recoverability	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.2-POF11	Considers Data Recoverability	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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.	5	
A1.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.3-POF1	Implements Business Continuity Plan Testing	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	10	
A1.3-POF2	Tests Integrity and Completeness of Backup	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.3-POF2		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
A1.3-POF2	Completeness of Backup Data	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		BCD-11.1	process, as well as the integrity and availability of the data.	5	



Secure Controls Framework (SCF) 2 of 4

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
A1.3-POF2		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	(optional) 5	
C1.1	Data N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
C1.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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.	5	
C1.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
C1.1-POF1	Defines and Identifies Confidential information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5	
C1.1-POF1	Defines and Identifies Confidential information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
C1.1-POF2	Retains Confidential Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
C1.1-POF2	Retains Confidential Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
C1.1-POF3	Protects Confidential Information From	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	10	
C1.1-POF3	Protects Confidential Information From Destruction	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (I) Retain Personal Lota (PD), including metadata, for an organization-defined time period to fulfill the purposely identified in the notice or as required by law; (2) bispose of, detroys, erasea, and/or anonymizes the Po, regardieso of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and anchived records).	5	
C1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information. Mechanisms exist to retain event logs for a time period consistent with records	10	
C1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Event Log Retention	MON-10	recommisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5	
C1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the upproase) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
C1.2-POF1	Identifies Confidential Information for	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (I) Retain Pernoul Lota (PD), including metadata, for an organization-defined time period to fulfill the purposely identified in the notice or as required by law; (2) Bispose of, detroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and anchived records).	5	
C1.2-POF2	Destroys Confidential Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
C1.2-POF2	Destroys Confidential	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
C1.2-POF2	Destroys Confidential	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to	5	
C1.2-POF2	Information Destroys Confidential	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Information Disposal	DCH-21	disposal, release out of organizational control or release for reuse. Mechanisms exist to securely dispose of, destroy or erase information.	5	
C1.2-P0F2	Destroys Confidential Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time perior do fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and anchived records).	5	
CC1.1	COSO Principle 1	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Cybersecurity & Data Protection Governance Program Cybersecurity & Data	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to provide a cybersecurity and data protection controls oversight	10	
CC1.1	COSO Principle 1	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection Controls Oversight	CPL-02	function that reports to the organization's executive leadership.	5	
CC1.1	COSO Principle 1	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	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 and data protection program.	5	
CC1.1	COSO Principle 1	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.1	COSO Principle 1	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work.	5	
CC1.1	COSO Principle 1	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
CC1.1	COSO Principle 1	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is	5	
CC1.1-POF1	Sets the Tone at the Top	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Cybersecurity & Data Protection Governance	GOV-01	reasonable assurance that a policy has been violated. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
					Program		Protection governance controls. Mechanisms exist to incorporate cybersecurity and data protection principles into		
CC1.1-POF1	Sets the Tone at the Top	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Business As Usual (BAU) Secure Practices	GOV-14	Business As Usual (BAU) practices through executive leadership involvement.	10	
CC1.1-POF1	Sets the Tone at the Top	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.1-POF2	Establishes Standards of Conduct	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC1.1-POF3	Evaluates Adherence to Standards of Conduct	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection	10	
CC1.1-POF3	Standards of Conduct Evaluates Adherence to Standards of Conduct	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Cybersecurity & Data Protection Controls Oversight	CPL-02	program measures of performance. Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	10	
CC1.1-POF3	Evaluates Adherence to Standards of Conduct	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements.	5	
CC1.1-POF3	Evaluates Adherence to Standards of Conduct	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.1-POF4	Addresses Deviations in a Timely Manner	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Personnel Sanctions	HRS-07	mitization actions. Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
CC1.1-POF4	Addresses Deviations in a Timely Manner	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
CC1.1-POF5	Considers Contractors and Vendor Employees in Demonstrating Its Commitment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC1.1-POF5	Considers Contractors and Vendor Employees in Demonstrating Its	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and	5	
CC1.1-POF5	Commitment Considers Contractors and Vendor Employees in Demonstrating Its Commitment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	IN Tela manageriate amodification setions to minimize the conscientiate amount of Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
CC1.1-POF5	Considers Contractors and Vendor Employees in Demonstrating Its	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed	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 and data protection controls between lateral elabelation and Extensive Section Production (SPER)	5	
	Commitment				(RASCI) Matrix		internal stakeholders and External Service Providers (ESPs).		



Secure Controls Framework (SCF) 3 of

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CC1.1-POF5	Considers Contractors and Vendor Employees in Demonstrating Its	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC1.2	COSO Principle 2	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	5	
CC1.2	COSO Principle 2	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	10	
CC1.2	COSO Principle 2	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Measures of Performance	GOV-05	regular basis. Mechanisms exist to develop, report and monitor cybersecurity and data protection	5	
CC1.2	COSO Principle 2	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Key Performance Indicators (KPIs)	GOV-05.1	program measures of performance. Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring and trend analysis	5	
CC1.2	COSO Principle 2	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Key Risk Indicators (KRIs)	GOV-05.2	of the cybersecurity and data protection program. Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the	5	
CC1.2	COSO Principle 2	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Position Categorization	HRS-02	cybersecurity and data protection program. Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those	5	
CC1.2	COSO Principle 2	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	positions. Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
CC1.2	COSO Principle 2	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC1.2-POF1	Establishes Oversight Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC1.2-POF1	Establishes Oversight Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	
CC1.2-POF1	Establishes Oversight Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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.	5	
CC1.2-POF1	Establishes Oversight Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
CC1.2-POF1	Establishes Oversight Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	5	
CC1.2-POF1	Establishes Oversight Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Governance	GOV-10	Mechanisms exist to facilitate data governance to oversee the organization's policies, standards and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and	5	
CC1.2-POF1	Establishes Oversight Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	contractual obligations. Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.2-POF1	Establishes Oversight Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 applicace.	5	
CC1.2-POF1	Establishes Oversight Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	positions. Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
CC1.2-POF2	Applies Relevant Expertise	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisma 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	
CC1.2-POF2	Applies Relevant Expertise	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.2-POF2	Applies Relevant Expertise	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC1.2-POF2	Applies Relevant Expertise	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
CC1.2-POF2	Applies Relevant Expertise	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC1.2-POF3	Operates Independently	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
CC1.2-POF3	Operates Independently	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	regular basis. Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.2-POF3	Operates Independently	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC1.2-POF4	Supplements Board Expertise	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 hasis	5	
CC1.2-POF4	Supplements Board Expertise	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.2-POF4	Supplements Board Expertise	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC1.2-POF4	Supplements Board Expertise	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC1.3	COSO Principle 3	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	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 and data protection program.	5	
CC1.3	COSO Principle 3	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
CC1.3	COSO Principle 3	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authoritative Chain of Command	GOV-04.2	and 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	5	
CC1.3	COSO Principle 3	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	managing data and technology-related risks. Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
CC1.3	COSO Principle 3	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC1.3	COSO Principle 3	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to again/zational operations, assets, individuals and other organizations; and (2) information protection needs a rising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
CC1.3-POF1	Considers All Structures of the Entity	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 resular basis.	5	
CC1.3-POF1	Considers All Structures of the Entity	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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.	5	
CC1.3-POF1	Considers All Structures of the Entity	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to	5	
CC1.3-POF2	Establishes Reporting Lines	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1	managing data and technology-related risks. Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring	5	
CC1.3-POF2	Establishes Reporting Lines	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authoritative Chain of Command	GOV-04.2	and 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	5	
CC1.3-POF3	Defines, Assigns, and Limits Authorities and Responsibilities	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	managing data and technology-related risks. 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 results hashing.	5	
CC1.3-POF3	Defines, Assigns, and Limits Authorities and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1		5	
	Responsibilities		l	<u> </u>	Accountability Structure		and managing data and technology-related risks.	1	



Secure Controls Framework (SCF) 4 of 4

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
CC1.3-POF3	Defines, Assigns, and Limits Authorities and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authoritative Chain of	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of	(optional)	
CC1.3-POF3	Responsibilities Defines, Assigns, and Limits Authorities and	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Command Defined Roles &	HRS-03	communication to remove ambiguity from individuals and teams related to managing data and technology-related risks. Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
001.01010	Responsibilities Defines Assigns and	COMMONDATION AS THE CONTROL OF THE LOCAL PROPERTY OF THE CONTROL T	Tunctional	inciscots with	Responsibilities Responsible,	1110 00	Mechanisms exist to document and maintain a Responsible, Accountable,		
CC1.3-POF3	Limits Authorities and Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	
CC1.3-POF4	Addresses Specific Requirements When Defining Authorities and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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.	5	
CC1.3-POF4	Addresses Specific Requirements When Defining Authorities and Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
CC1.3-POF4	Addresses Specific Requirements When Defining Authorities and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
CC1.3-POF4	Addresses Specific Requirements When Defining Authorities and Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection controls between	5	
CC1.3-POF5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1	Internal stakeholders and 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 managing data and technology-related risks.	5	
CC1.3-POF5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
CC1.3-POF5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
CC1.3-POF5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed	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 and data protection controls between	5	
CC1.3-POF6	Establishes Structures, Reporting Lines, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(RASCI) Matrix Stakeholder Accountability Structure	GOV-04.1	internal stakeholders and 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	5	
	Authorities to Support Establishes Structures, Reporting Lines, and				, , , , , , , , , , , , , , , , , , , ,		and 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		
CC1.3-POF6	Authorities to Support Compliance With Legal and Contractual Privacy Requirements	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC1.3-POF6	Establishes Structures, Reporting Lines, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.3-POF6	Authorities to Support Establishes Structures, Reporting Lines, and Authorities to Support	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed (awtully, fairly and transparently.	5	
CC1.3-POF6	Establishes Structures, Reporting Lines, and Authorities to Support	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	5	
CC1.4	COSO Principle 4	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
CC1.4	COSO Principle 4	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity and data protection programs and document all exceptions to this requirement.	5	
CC1.4	COSO Principle 4	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 / initiatives.	5	
CC1.4	COSO Principle 4	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection-Minded Workforce Continuing Professional	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls. Mechanisms exist to ensure cybersecurity and data protection personnel receive	5	
CC1.4	COSO Principle 4	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Education (CPE) - Cybersecurity & Data Protection Personnel	SAT-03.7	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	
CC1.4-POF1	Establishes Policies and Practices	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	10	
CC1.4-POF1	Establishes Policies and Practices	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.4-POF2	Evaluates Competence and Addresses Shortcomings	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 (Al) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	5	
CC1.4-POF2	Evaluates Competence and Addresses Shortcomings	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Al & Autonomous Technologies Stakeholder Competencies	AAT-13.1	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related operator and practitioner proficiency requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT) are defined, assessed and documented.	5	
CC1.4-POF2	Evaluates Competence and Addresses	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.4-POF2	Shortcomings Evaluates Competence and Addresses	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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-POF2	Shortcomings Evaluates Competence and Addresses	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Competency Requirements for Security-	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
CC1.4-POF2	Shortcomings Evaluates Competence and Addresses	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Related Positions Identify Critical Skills &	HRS-13	Mechanisms exist to evaluate the critical cybersecurity and data protection skills	5	
CC1.4-POF2	Shortcomings Evaluates Competence and Addresses	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Gaps Third-Party Management	TPM-01	needed to support the organization's mission and identify gaps that exist. Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC1.4-POF2	Shortcomings Evaluates Competence and Addresses	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity	5	
CC1.4-POF3	Shortcomings Attracts, Develops, and Retains Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Robust Stakeholder Engagement for Al & Autonomous	AAT-11	and data protection controls. 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	
CC1.4-POF3	Attracts, Develops, and Retains Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Technologies Al & 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	
CC1.4-POF3	Attracts, Develops, and Retains Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.4-POF3	Attracts, Develops, and Retains Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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		Functional	intersects with	Identify Critical Skills &	HRS-13	Mechanisms exist to evaluate the critical cybersecurity and data protection skills	5	
CC1.4-POF3 CC1.4-POF3	Retains Individuals Attracts, Develops, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	intersects with	Gaps Cybersecurity & Data Protection-Minded	HRS-13 SAT-01	needed to support the organization's mission and identify gaps that exist. Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
CC1.4-POF3	Retains Individuals Attracts, Develops, and		Functional	intersects with	Workforce Continuing Professional Education (CPE) -		Mechanisms exist to ensure cybersecurity and data protection personnel receive Continuing Professional Education (CPE) training to maintain currency and	5	
	Retains Individuals Attracts, Develops, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.			Cybersecurity & Data Protection Personnel	SAT-03.7	proficiency with industry-recognized secure practices that are pertinent to their assigned roles and responsibilities. Mechanisms exist to facilitate the implementation of third-party management		
CC1.4-POF3	Retains Individuals Attracts, Develops, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management Review of Third-Party	TPM-01	controls. Mechanisms exist to monitor, regularly review and assess External Service Providers	5	
CC1.4-POF3	Retains Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Services	TPM-08	(ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls. Mechanisms exist to evaluate the critical cybersecurity and data protection skills	5	
CC1.4-POF4	Plans and Prepares for Succession Plans and Prepares for	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identify Critical Skills & Gaps Perform Succession	HRS-13 4	needed to support the organization's mission and identify gaps that exist. Mechanisms exist to perform succession planning for vital cybersecurity and data	5	
CC1.4-POF4	Succession	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Planning	HRS-13.4	protection roles.	5	



Secure Controls Framework (SCF) 5 of 4

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CC1.4-POF5	Considers the Background of Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	
CC1.4-POF6	Considers the Technical Competency of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
	Individuals Considers the Technical				Competency		Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.		
CC1.4-POF6	Competency of Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Requirements for Security- Related Positions	HRS-03.2		10	
CC1.4-POF7	Provides Training to Maintain Technical Competencies	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection 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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and	5	
CC1.4-POF7	Provides Training to Maintain Technical	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Continuing Professional Education (CPE) - Cybersecurity & Data	SAT-03.7	Annually thereafter. Mechanisms exist to ensure cybersecurity and data protection personnel receive Continuing Professional Education (CPE) training to maintain currency and	5	
CC1.4-POF7	Provides Training to Maintain Technical	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection Personnel Continuing Professional Education (CPE) - DevOps	SAT-03.8	proficiency with industry-recognized secure practices that are pertinent to their assigned roles and reconstibilities. Mechanisms exist to ensure application development and operations (DevOps) personnel receive Continuing Professional Education (CPE) training on Secure	5	
	Competencies				Personnel		Software Development Practices (SSDP) to appropriately address evolving threats. Mechanisms exist to develop, report and monitor cybersecurity and data protection		
CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Measures of Performance Key Performance	GOV-05	program measures of performance. Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs)	5	
CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Indicators (KPIs)	GOV-05.1	to assist organizational management in performance monitoring and trend analysis of the cybersecurity and data protection program. Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist	5	
CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Key Risk Indicators (KRIs)	GOV-05.2	senior management in performance monitoring and trend analysis of the cybersecurity and data protection program.	5	
CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Non-Compliance Oversight	CPL-01.1	statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar conflidentiality agreements that reflect the needs to protect data and operational details. or both employees and third-parties.	5	
CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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. Mechanisms exist to adjust logical and physical access authorizations to Technology	5	
CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Personnel Transfer	HRS-08	Mechanisms exist to adjust togical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer. In a timely manner.	5	
CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Asset Collection	HRS-09.1	Mechanisms exist to retrieve organization-owned assets upon termination of an individual's employment.	5	
CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	High-Risk Terminations	HRS-09.2	Mechanisms exist to expedite the process of removing "high risk" individual's access to Technology Assets, Applications, Services and/or Data (TAASD) upon termination, as determined by management.	5	
CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Post-Employment Requirements Notification	HRS-09.3	Mechanisms exist to govern former employee behavior by formally notifying terminated individuals of their applicable, legally binding post-employment requirements for the protection of sensitive/regulated data.	5	
CC1.5-POF1	Enforces Accountability Through Structures, Authorities, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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.	5	
CC1.5-POF1	Enforces Accountability Through Structures, Authorities, and Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
CC1.5-POF1	Enforces Accountability Through Structures, Authorities and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
CC1.5-POF2	Establishes Performance Measures, Incentives, and Rewards	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5	
CC1.5-POF2	Establishes Performance Measures, Incentives, and Rewards	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
CC1.5-POF3	Evaluates Performance Measures, Incentives, and Rewards for Ongoing	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
CC1.5-POF3	Relevance Evaluates Performance Measures, Incentives, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	regular basis. Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.5-P0F4	Rewards for Ongoing Considers Excessive Pressures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Steering Committee &	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business adignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a	10	
CC1.5-POF4	Pressures Considers Excessive		Functional	Interne	Program Oversight Human Resources	HRS-01	cybersecurity, data privacy and business executives, which meets formally and on a regular basis. Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.5-PUF4	Pressures Evaluates Performance	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	runctionat	intersects with	Security Management	rino-UI	Mechanisms exist to coordinate cybersecurity, data protection and business	•	
CC1.5-POF5	and Rewards or Disciplines Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Steering Committee & Program Oversight	GOV-01.1	alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular hasis. Mechanisms exist to develop, report and monitor cybersecurity and data protection.	10	
CC1.5-POF5	Evaluates Performance and Rewards or Disciplines Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Measures of Performance	GOV-05	program measures of performance.	5	
CC1.5-POF5	Evaluates Performance and Rewards or Disciplines Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.5-POF5	Evaluates Performance and Rewards or Disciplines Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Takes Disciplinary Actions	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	10	
CC2.1	COSO Principle 13	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5	
CC2.1	COSO Principle 13	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
CC2.1	COSO Principle 13	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	
CC2.1	COSO Principle 13	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 check for Redundant, Obsolete/Outdated, Toxic or Trivial	5	
CC2.1	COSO Principle 13	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Quality Operations	DCH-22	(ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information across the information lifecycle.	5	
CC2.1	COSO Principle 13	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 sexpelfic noise of the proposes area.	5	
CC2.1-POF1	Identifies Information Requirements	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Define Control Objectives	GOV-09	standards to achieve the specific goals of the process area. Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5	
	gunoniento		<u> </u>	1	I .	l	I	l	<u> </u>



Secure Controls Framework (SCF) 6 of 4

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
CC2.1-POF1	Identifies Information Requirements	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each system, application and/or service under their control.	(optional) 5	
CC2.1-POF1	Identifies Information Requirements	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 appellic results of the numbers area.	5	
CC2.1-POF2	Captures Internal and External Sources of Data	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each system, application and/or service under their control.	5	
CC2.1-POF2	Captures Internal and External Sources of Data	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5	
CC2.1-POF2	Captures Internal and External Sources of Data	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 cools of the process area.	5	
CC2.1-POF3	Processes Relevant Data Into Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each system, application and/or service under their control.	5	
CC2.1-POF3	Processes Relevant Data Into Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 seceptic coals of the process area.	5	
CC2.1-POF4	Maintains Quality Throughout Processing	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compet data and/or process owners to operationalize cybersecurity and data protection practices for each system, application and/or service under their control.	5	
CC2.1-POF4	Maintains Quality Throughout Processing	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 de-identification of information across the information lifecycle.	5	
CC2.1-POF4	Maintains Quality Throughout Processing	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5	
CC2.1-POF4	Maintains Quality Throughout Processing	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 seceptic coals of the process area.	5	
CC2.1-POF5	Documents Data Flow	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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. Mechanisms exist to maintain network architecture diagrams that:	5	
CC2.1-POF5	Documents Data Flow	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	(1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	10	
CC2.1-POF6	Manages Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC2.1-POF6	Manages Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (FASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization defined information deemed necessary to achieve effective property accountability; and (5) is available for review and audit by designated organizations) personnel.	5	
CC2.1-POF6	Manages Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Automated Location Tracking	AST-02.10	Mechanisms exist to track the geographic location of system components.	5	
CC2.1-POF6	Manages Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC2.1-POF6	Manages Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
CC2.1-POF6	Manages Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 (ICIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
CC2.1-POF7	Classifies Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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. Mechanisms exist to reclassify data, including associated Technology Assets,	10	
CC2.1-POF7	Classifies Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Reclassification	DCH-11	Applications and/or Services (TAAS), commensurate with the security category and/or classification level of the information. Mechanisms exist to determine cybersecurity and data protection control	5	
CC2.1-POF7	Classifies Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Asset Scope Classification	AST-04.1	applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5	
CC2.1-POF8	Uses Information That Is Complete and Accurate	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	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 de-identification of information across the information lifecycle.	10	
CC2.1-POF9	Manages the Location of Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC2.1-POF9	Manages the Location of Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TASD) that: (1) Accurately reflects the current TASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization defined information deemed necessary to schiws effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
CC2.1-POF9	Manages the Location of Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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-POF9	Manages the Location of Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Automated Location Tracking	AST-02.10	Mechanisms exist to track the geographic location of system components.	5	
CC2.1-POF9	Manages the Location of Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC2.1-POF9	Manages the Location of Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
CC2.1-POF9	Manages the Location of Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC2.1-POF9	Manages the Location of Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC2.1-POF9	Manages the Location of Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC2.1-POF9	Manages the Location of Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection controls oversight	5	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection Controls Oversight	CPL-02	function that reports to the organization's executive leadership.	5	



Secure Controls Framework (SCF) 7 of

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	(optional) 5	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection program.	5	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection program.	5	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Operations Security Standardized Operating	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls. Mechanisms exist to identify and document Standardized Operating Procedures	5	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Procedures (SOP) Cybersecurity & Data	OPS-01.1	(SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks. Mechanisms exist to facilitate the implementation of cybersecurity and data	5	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection Portfolio Management	PRM-01	protection-related resource planning controls that define a viable plan for achieving cybersecurity and data protection objectives. Mechanisms exist to identify critical system components and functions by	5	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Requirements Definition	PRM-05	precrains a seas to be many critical system components and binctions by performing a critically analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle ISDLCI. Mechanisms exist to facilitate the implementation of industry-recognized	5	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Engineering Principles	SEA-01	cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Standardized Terminology Publishing Cybersecurity	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments. Mechanisms exist to establish, maintain and disseminate cybersecurity and data	5	
CC2.2-POF1	Communicates Internal Control Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	& Data Protection Documentation	GOV-02	protection policies, standards and procedures.	5	
CC2.2-POF1	Communicates Internal Control Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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-POF1	Communicates Internal Control Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC2.2-POF2	Communicates With the Board of Directors	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection program.	10	
CC2.2-POF3	Provides Separate Communication Lines	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC2.2-POF3	Provides Separate Communication Lines	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data	5	
CC2.2-POF3	Provides Separate Communication Lines	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	protection-related incidents. Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake:	5	
CC2.2-POF4	Selects Relevant Method of Communication	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
CC2.2-POF4	Selects Relevant Method of Communication	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Contacts With Authorities	GOV-06	regular basis. Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5	
							Mechanisms exist to establish contact with selected groups and associations within the cybersecurity and data protection communities to: (1) Facilitate ongoing cybersecurity and data protection education and training for		
CC2.2-P0F4	Selects Relevant Method of Communication	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Contacts With Groups & Associations	GOV-07	organizational personnel; (2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and (3) Share current cybersecurity and/or data privacy-related information including throats, autionabilities and incidential.	5	
CC2.2-POF5	Communicates Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
CC2.2-POF5	Communicates Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection controls between internal stakeholders and Extema Service Providers (ESPs).	5	
CC2.2-POF6	Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (j) Peparation; (z) Automated event detection or manual incident report intake; (g) Analysis; (4) Containment; (6) Eradiscition; and	5	
CC2.2-POF6	Communicates Information on Reporting Failures, Incidents, Concerns, and Other	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	IRI Benzimer Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5	
CC2.2-POF6	Matters Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	
CC2.2-POF6	Communicates Information on Reporting Failures, Incidents, Concerns, and Other	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
CC2.2-POF6	Matters Communicates Information on Reporting Failures, Incidents, Concerns, and Other	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC2.2-POF6	Matters Communicates Information on Reporting Failures, Incidents, Concerns, and Other	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC2.2-POF7	Matters Communicates Objectives and Changes to Objectives	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	
CC2.2-POF7	Communicates Objectives and Changes to Objectives	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
CC2.2-POF7	Communicates Objectives and Changes to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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-POF8	Objectives Communicates Information to Improve	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection-Minded	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
CC2.2-POF8	Security Knowledge and Communicates Information to Improve Security Knowledge and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Workforce Cybersecurity & Data Protection 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	
CC2.2-POF8	Awareness Communicates Information to Improve Security Knowledge and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity and data protection swareness training that is current and relevant to the cyber threats that users might encounter in day, to, day business operations.	5	
CC2.2-POF9	Awareness Communicates Information to Improve	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Sensitive / Regulated Data Storage, Handling &	SAT-03.3	encounter in day-to-day business operations. Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive / regulated data is formally trained in data handling	5	
CC2.2-POF9	Privacy Knowledge and Communicates Information to Improve	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Processing Privileged Users	SAT-03.5	requirements. Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities	5	
	Privacy Knowledge and	(,							



Secure Controls Framework (SCF) 8 of

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
CC2.2-POF9	Communicates Information to Improve Privacy Knowledge and Awareness	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	
CC2.2-POF9	Communicates Information to Improve Privacy Knowledge and Awareness	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	
CC2.2-POF9	Communicates Information to Improve Privacy Knowledge and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
CC2.2-POF10	Communicates Incident Reporting Methods	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	5	
CC2.2-POF10	Communicates Incident Reporting Methods	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
CC2.2-POF10	Communicates Incident Reporting Methods	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (8) Renowery	5	
CC2.2-POF10	Communicates Incident Reporting Methods Communicates Incident	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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. Mechanisms exist to maintain and make available a current and viable incident	5	
CC2.2-POF10 CC2.2-POF11	Reporting Methods Communicates Information About System	Download AICPA's Trust Services Criteris (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Plan (IRP) Asset Scope Classification	IRO-04 AST-04.1	rectnations easi to determine cybersecurity and data protection continued. Response Plan (RP) to all stakeholders. Mechanisms exist to determine cybersecurity and data protection control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and	5	
CC2.2-POF11	Operation and Boundaries Communicates Information About System Operation and Boundaries	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Control Applicability Boundary Graphical Representation	AST-04.2	personnel (internal and third-parties). Mechanisms exist to ensure control applicability is appropriately-determined for Technology Assets, Applications and/or Services (TAAS) and third parties by graphically representing applicable boundaries.	5	
CC2.2-POF11	Communicates Information About System Operation and Boundaries	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
CC2.2-POF11	Communicates Information About System Operation and Boundaries	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 confloratibility, integrity, vanilability and setly of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	5	
CC2.2-POF11	Communicates Information About System Operation and Boundaries	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or simitar document repositories, to identify and maintain key architectural information on each critical Technology Assets, Applications and/or Services (TAAS), as well as influence inputs, entities and TAAS, providing a historical record of the data and its origins.	5	
CC2.2-POF12	Communicates System Objectives	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC2.2-POF12	Communicates System Objectives	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
CC2.2-POF12	Communicates System Objectives	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection 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	
CC2.2-POF12	Communicates System Objectives	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annualty thereafter,	5	
CC2.2-POF13	Communicates System Changes Communicates System	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	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.	5	
CC2.2-POF13	Changes Communicates System	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Change Control Stakeholder Notification	CHG-02	Mechanisms exist to govern the technical configuration change control processes. Mechanisms exist to ensure stakeholders are made aware of and understand the	5	
CC2.2-POF13	Changes Communicates System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	of Changes Role-Based Cybersecurity & Data Protection Training	CHG-05 SAT-03	impact of proposed changes. Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties;	5	
CC2.2-P0F13	Communicates System Changes	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Suspicious Communications & Anomalous System	SAT-03.2	(2) When required by system changes; and (3) Annually threafter. Mechanisms exist to provide training to personnel on organization-defined indicators of matware to recognize suspicious communications and anomalous behavior.	5	
CC2.3	COSO Principle 15	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Behavior Statutory, Regulatory &	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant	5	
CC2.3	COSO Principle 15	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Contractual Compliance Cybersecurity & Data Protection Controls	CPL-02	statutory, regulatory and contractual controls. Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	5	
CC2.3	COSO Principle 15	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Oversight Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law	5	
CC2.3	COSO Principle 15	Download ACPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Contacts With Groups & Associations	GOV-07	enforcement and regulatory bodies. Mechanisms exist to establish contact with selected groups and associations within the cybersecurity and data protection communities to: (1) Facilitate onging cybersecurity and data protection education and training for organizational personnel; (2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and (3) Share current cybersecurity and/or data privacy-related information including thmass. submarkilities and incidents.	5	
CC2.3	COSO Principle 15	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
CC2.3	COSO Principle 15	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 document Personal Data (PD) processing activities that cover	5	
CC2.3	COSO Principle 15	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Documenting Data Processing Activities	PRI-14	collecting, receiving, processing, storing, transmitting, updating, sharing and disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements. Mechanisms exist to timely-report incidents to applicable:	5	
CC2.3-POF1	Communicates to External Parties	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	(2) Affected clients & third-parties; and (3) Regulatory authorities. Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
CC2.3-POF1	Communicates to External Parties	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to provide cybersecurity and data protection incident information	5	
CC2.3-POF1	Communicates to External Parties	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Coordination	IRO-10.4	rectains the state of provide cyters excurry and use protection finder intimidation to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to the incident. Mechanisms exist to establish a direct, cooperative relationship between the	5	
CC2.3-POF2	Enables Inbound Communications	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Coordination With External Providers	IRO-11.2	organization's incident response capability and external service providers.	5	
CC2.3-POF2	Enables Inbound Communications	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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, worldorce, and/or customers based on industry-recognized standards to achieve the secetic acosts of the process area.	5	
CC2.3-POF2	Enables Inbound Communications	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
CC2.3-POF3	Communicates With the Board of Directors	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybensecurity, 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. Mechanisms exist to provide governance oversight reporting and recommendations	5	
CC2.3-POF3	Communicates With the Board of Directors	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program.	5	
CC2.3-POF4	Provides Separate Communication Lines	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	



Secure Controls Framework (SCF) 9 of 4

	FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Company	CC2.3-POF4		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Workplace Investigations	HRS-07.1		5	
Part	CC2.3-POF5	Selects Relevant Method	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection Governance	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data	5	<u> </u>
	CC2.3-POF5		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Status Reporting To	GOV-01.2	to those entrusted to make executive decisions about matters considered material to	5	
Manufacture	CC2.3-POF5		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CPL-01	statutory, regulatory and contractual controls.	5	
Company	CC2.3-POF6	Related to Confidentiality and Changes to Those	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	(Business Process	OPS-03	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	5	
Column	CC2.3-POF6	Related to Confidentiality and Changes to Those	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to	5	
March Marc	CC2.3-POF6	Related to Confidentiality and Changes to Those	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Accountable, Supportive, Consulted & Informed	TPM-05.4	Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between	5	
Company Comp	CC2.3-POF7	Related to Privacy and Changes to Those	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Privacy Program	PRI-01	controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are	5	
Part	CC2.3-POF7	Related to Privacy and Changes to Those	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Privacy Notice	PRI-02	(I) Make data privary notice(s) available to individuals upon first interacting with an organization and subsequently as necessary. (2) Ensure that data privary notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related orteria required by applicable statutory, regulatory and contractual obligations. (4) Define the acops of PD processing activities, including the geographic locations and third-party recipients that process the PD within the acops of the data privacy notice; (6) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention	5	
Column	CC2.3-POF7	Related to Privacy and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		TPM-05	protection requirements with third-parties, reflecting the organization's needs to	5	
	CC2.3-POF8	Objectives Communicates Incident	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	(1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (6) Eradicition; and	5	
Control Cont	CC2.3-POF8		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IRO-04	Mechanisms exist to maintain and make available a current and viable Incident	5	
Columbia	CC2.3-POF8		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution	5	
Control Cont	CC2.3-POF8		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
Column	CC2.3-POF9	Information About System	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of		IAO-03	document repositories, to identify and maintain key architectural information on each critical Technology Assets, Applications and/or Services (TAAS), as well as influence inputs, entities and TAAS, providing a historical record of the data and its	10	
Communication Communicatio	CC2.3-POF9	Information About System	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management	10	
CC13-P0F11 Commission Significant Commission of the Commission Significant Commission of the Commission Significant Commission Significan	CC2.3-POF9	Communicates Information About System	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Accountable, Supportive, Consulted & Informed	TPM-05.4	Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	10	
CC3 P0F19 Communicate Spring Contraction Spring Contraction Contraction Spring Contraction	CC2.3-POF10		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IAO-03	document repositories, to identify and maintain key architectural information on each critical Technology Assets, Applications and/or Services (TAAS), as well as influence inputs, entitles and TAAS, providing a historical record of the data and its origins.	5	
COL 3 FOTTS Office Minimization System Control (TA) To trigenths control wording. Purchased in the Park Control (TA) To t	CC2.3-POF10		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		TDA-01	acquisition strategies, contract tools and procurement methods to meet unique	5	
COL3-POF11 Communicates System Description ACOVAS Trust Services Criteria (TSC) for specific control wording. COL3-POF11 Communicates System Representatives where the Color of TSC) for specific control wording. COL3-POF11 Communicates System Representatives where the Color of TSC) for specific control wording. COL3-POF11 Communicates System Representatives where the Color of TSC) for specific control wording. COL3-POF11 Communicates System Representatives where the Color of TSC) for specific control wording. COL3-POF11 Communicates System Representatives where the Color of TSC) for specific control wording. COL3-POF11 Communicates System Representatives and Color of the Color of TSC) for specific control wording. COL3-POF11 Communicates System Representatives and Color of the Color of TSC) for specific control wording. COL3-POF12 Communicates System Representatives and Color of TSC) for specific control wording. COL3-POF12 Communicates System Representatives and Color of TSC) for specific control wording. COL3-POF12 Communicates System Representatives System Representatives and Color of TSC) for specific control wording. COL3-POF12 Communicates System Representatives System Representatives and Color of TSC) for specific control wording. COL3-POF12 Communicates System Representatives System Representatives and Color of TSC) for specific control wording. COL3-POF12 Communicates System Representatives System Representatives System Representatives and Color of TSC) for specific control wording. COL3-POF12 Communicates System Representatives System Re	CC2.3-POF10		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC2.3-POF11 Communicates System Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CC2.3-POF12 Communicates System Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CC2.3-POF12 Communicates System Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CC2.3-POF12 Communicates System Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CC2.3-POF12 Communicates System Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CC2.3-POF12 Services System Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CC2.3-POF12 Services System Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CC2.3-POF12 Services System Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CC2.3-POF12 Services System Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CC2.3-POF12 Services System Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CC2.3-POF12 Services System Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CC2.3-POF12 Services System Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CC2.3-POF12 Services System Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CC2.3-POF12 Services System Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CC2.3-POF12 Services System Developed System Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CC2.3-POF12 Services System Developed System	CC2.3-POF10		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		TPM-05	protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
CC2.3 POPT1 CC2.3	CC2.3-POF11		Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with		IAO-03	document repositories, to identify and maintain key architectural information on each critical Technology Assets, Applications and/or Services (TAAS), as well as influence inputs, entities and TAAS, providing a historical record of the data and its origins.	5	
CC3.9F0F12 Communicates System Responsibility of Responsibility Communicates System Re	CC2.3-POF11		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Requirements	TPM-05	protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
CC2.3-POF12 Information net Reporting System Failures. CC2.3-POF12 CC2.3-POF12 Information on Reporting System Failures. CC2.3-POF12 Information net Reporting System Failures.	CC2.3-POF11	Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Accountable, Supportive, Consulted & Informed	TPM-05.4	Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	10	
CC2.3-POF12 CC3.4 POF12 CC2.3-POF12 CC3.4 POF12 CC3.4 POF12 CC3.4 POF12 CC3.4 POF12 CC3.4 POF12 CC3.5	CC2.3-POF12	Information on Reporting	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
Information on Reporting System Fallures, Incidents, Concerns, and Officents, Concerns, and Offi	CC2.3-POF12	Communicates Information on Reporting System Failures.	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	External Providers	IRO-11.2	organization's incident response capability and external service providers.	5	
CC2.3-POF12 Information on Reporting System Failures, Incidents, Concerns, and Other Matters CC2.3-POF12 System Failures, Incidents, Concerns,	CC2.3-POF12	Information on Reporting System Failures, Incidents, Concerns, and Other Matters	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Communications & Anomalous System	SAT-03.2		5	
C2.3-POF12 System Failures, Incidents, Connumicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters C2.3-POF12 System Failures, Incidents System Failures, Incidents, Concerns,	CC2.3-POF12	Information on Reporting	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01		5	
CC2.3-POF12 CC3.1 COSO Principle 6 COmmunicates Information on Reporting System Failures, Inclients, Concerns, and Other Matters CC3.1 COSO Principle 6 CC3.1 COSO Principle 7 CC3.1 COSO Principle 7 CC3.1 COSO Principle 7 CC3.1 COSO Principle 7 CC3.1 COSO Princip	CC2.3-POF12	Communicates Information on Reporting System Failures, Incidents, Concerns, and	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with		TPM-05	protection requirements with third-parties, reflecting the organization's needs to	5	
CC2.3-POF12 CC3.1 COSO Principle 6 CC3.1 COSO Principle 7 CC4.1 COSO Principle 7 CC4.1 COSO Principle 7 CC4.1 COSO Princi	CC2.3-POF12	Communicates Information on Reporting System Failures, Incidents, Concerns, and	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with		TPM-05.1	of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that	5	
CC3.1 CCSO Principle 6 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional subset of Define Control Objectives GOV-99 Implementation and management of the organization's implementation of objectives as the basis for the selection, implementation and management of the organization's implementation and management of the organization's implementation of objectives as the basis for the selection, implementation and management of the organization's implementation and management of the organization's implementation and management of the organization's implementation of objectives as the basis for	CC2.3-P0F12	Communicates Information on Reporting System Failures, Incidents, Concerns, and	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with		TPM-05.2		5	
CC3.1 COSO Principle 6 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Protection Portfolio PRM-01 protection-related resource planning controls that define a viable plan for achieving 5	CC3.1		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Define Control Objectives	GOV-09		10	
	CC3.1	COSO Principle 6	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PRM-01		5	



Secure Controls Framework (SCF) 10 of 4

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CC3.1	COSO Principle 6	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection In Project	PRM-04	Mechanisms exist to assess cybersecurity and data protection 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	5	
					Management		meeting the requirements. Mechanisms exist to define business processes with consideration for cybersecurity		
CC3.1	COSO Principle 6	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and	5	
					Definition		(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is		
CC3.1	COSO Principle 6	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Management Program	RSK-01	Abtained Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
CC3.1	COSO Principle 6	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal rechanged and account of the chain of th	5	
003.1	COSO PINICIPIE 6	DOWNLOAD AICEA'S ITUSE SERVICES CITICATA (1907) OF SPECIAL CONTROL WORKING.	runctional	intersects with	Management (SCRM) Plan	NSK-09	selected mitigating actions and monitoring performance against those plans.		
CC3.1	COSO Principle 6	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection principles that addresses risk to organizational operations, assets,	5	
	Reflects Management's						individuals, other organizations. Mechanisms exist to establish control objectives as the basis for the selection,		
CC3.1-POF1	Choices Reflects Management's	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Define Control Objectives Defining Business Context	GOV-09	Implementation and management of the organization's internal control system. Mechanisms exist to define the context of its business model and document the	5	
CC3.1-POF1	Choices	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	& Mission	GOV-08	organization's mission. Mechanisms exist to identify:	5	
CC3.1-POF1	Reflects Management's	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 	5	
	Choices						(4) Priorities, benefits and trade-offs considered by the organization for managing risk.		
CC3.1-POF1	Reflects Management's Choices	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
CC3.1-POF1	Reflects Management's Choices	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.1-POF1	Reflects Management's Choices	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.1-POF2	Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.1-POF2	Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.1-POF3	Includes Operations and Financial Performance	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission. Mechanisms exist to identify:	5	
	Includes Operations and						Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring;		
CC3.1-POF3	Financial Performance Goals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Framing	RSK-01.1	(3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing	5	
					Cybersecurity & Data		risk. Mechanisms exist to facilitate the implementation of cybersecurity and data		
CC3.1-POF4	Forms a Basis for Committing of Resources	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection Portfolio Management	PRM-01	protection-related resource planning controls that define a viable plan for achieving cybersecurity and data protection objectives.	5	
CC3.1-POF4	Forms a Basis for Committing of Resources	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 / initiatives.	5	
CC3.1-POF5	Complies With Applicable Accounting Standards	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Operationalizing Cybersecurity & Data	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each system, application and/or	5	
CC3.1-POF5	Complies With Applicable	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection Practices Statutory, Regulatory &	CPL-01	service under their control. Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
CC3.1-POF6	Accounting Standards Considers Materiality	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Contractual Compliance Materiality Determination	GOV-16	Mechanisms exist to define materiality threshold criteria capable of designating an	5	
							incident as material. Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring;		
CC3.1-POF6	Considers Materiality	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Framing	RSK-01.1	(2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and	5	
							(4) Priorities, benefits and trade-offs considered by the organization for managing fisk.		
CC3.1-POF6	Considers Materiality	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.1-POF7	Reflects Entity Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Service Delivery (Business Process	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	5	
	, , , , , , , , , , , , , , , , , , , ,				Support)		business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.		
							Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other		
CC3.1-POF7	Reflects Entity Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	(2) Information protection needs arising from the defined business processes and	5	
							revises the processes as necessary, until an achievable set of protection needs is obtained		
CC3.1-POF8	Complies With Externally Established Frameworks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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-POF8	Complies With Externally Established Frameworks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
	Complies With Externally				Service Delivery		Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning,		
CC3.1-POF8	Established Frameworks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(Business Process Support)	OPS-03	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	
							Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines:		
CC3.1-POF8	Complies With Externally Established Frameworks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	(1) The resulting risk to organizational operations, assets, individuals and other organizations; and	5	
							(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is antizined.		
CC3.1-POF9	Considers the Required Level of Precision	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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-POF9	Considers the Required Level of Precision	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
000 4 000-	Considers the Required	Doublood AICRA's Tour Senile - Criteria (CCC) to	Brookle 1	inter	Service Delivery	000	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning,	-	
CC3.1-POF9	Level of Precision	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(Business Process Support)	OPS-03	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 anals of the process area.	5	
							Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines:		
CC3.1-POF9	Considers the Required Level of Precision	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	(1) The resulting risk to organizational operations, assets, individuals and other organizations; and	5	
							(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.		
CC3.1-POF10	Reflects Entity Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 companying of the protection and protections.	5	
CC3.1-POF10	Reflects Entity Activities		Functional	intersects with	Contacts With Authorities	GOV-06	the organization's cybersecurity and data protection program. Mechanisms exist to identify and document appropriate contacts with relevant law	5	
CC3.1-POF10			Functional	intersects with	Contacts With Authorities Cybersecurity & Data Protection Status	GOV-06 GOV-17	enforcement and regulatory bodies. Mechanisms exist to submit status reporting of the organization's cybersecurity	5	
CGS. 1-POF IU	Reflects Entity Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	runctional	intersects with	Reporting Reporting	GUV-1/	and/or data privacy program to applicable statutory and/or regulatory authorities, as required.		



Secure Controls Framework (SCF) 11 of 40

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CC3.1-POF10	Reflects Entity Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 originalization stethnology capabilities supporting business functions, worldroce, and/or customers based on industry-recognized standards to achieve the searcific ceads of the noncess area. Mechanisms exist to define business processes with consideration for cybersecurity	5	
CC3.1-POF10	Reflects Entity Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
CC3.1-POF11	Reflects Management's Choices	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.1-POF11	Reflects Management's Choices	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection program.	5	
CC3.1-POF11	Reflects Management's Choices	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governace and service management to ensure appropriate glorance 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 processes area. Mechanisms exist to define business processes with consideration for cybersecurity mechanisms exist to define business processes with consideration for cybersecurity.	5	
CC3.1-POF11	Reflects Management's Choices	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	and data protection that determines: (1) The resulting risk to againizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
CC3.1-POF12	Considers the Required Level of Precision	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 secetific socials of the process area.	5	
CC3.1-POF12	Considers the Required Level of Precision	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is inhitiation.	5	
CC3.1-POF13	Reflects Entity Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	And the control of th	5	
CC3.1-POF13	Reflects Entity Activities	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) information protection needs a rising from the defined business processes and reviews the processes as necessary, until an achievable set of protection needs is instance.	5	
CC3.1-POF14	Reflects External Laws and Regulations	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
CC3.1-POF14	Reflects External Laws and Regulations	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 sooils of the process area.	5	
CC3.1-POF14	Reflects External Laws and Regulations	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Intermediations; and (2) Intermediation protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is instanced.	5	
CC3.1-POF15	Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	5	
CC3.1-POF15	Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 nething the annual function of the numbers are Mechanisms exist to define business processes with consideration for cybersecurity	5	
CC3.1-POF15	Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	and data protection that determines: (1) The resulting risk to agrain/zational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is individuals.	5	
CC3.1-POF15	Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
CC3.1-POF15	Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.1-POF15	Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.1-POF16	Establishes Sub- Objectives for Risk Assessment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governace and service management to ensure appropriate glamping, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the assocific goals of the process area. Mechanisms exist to define business processes with consideration for cybersecurity declarations.	5	
CC3.1-POF16	Establishes Sub- Objectives for Risk Assessment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is ortenied.	5	
CC3.1-POF16	Establishes Sub- Objectives for Risk Assessment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
CC3.1-POF16	Establishes Sub- Objectives for Risk Assessment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Acotications, Services and/or Data TFASDI. Mechanisms exist to identify:	5	
CC3.2	Considers Tolerances for Risk	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Risk Framing	RSK-01.1	(1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Contartisms facting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-ofts considered by the organization for managing risk.	5	
CC3.2	Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	10	
CC3.2	Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset namer.	5	
CC3.2	Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
CC3.2	Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	



cure Controls Framework (SCF) 12 of 4

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CC3.2	Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 Technology Assets, Applications and/or Services (TAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
CC3.2	Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
CC3.2	Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
CC3.2-POF1	Includes Entity, Subsidiary, Division, Operating Unit, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
CC3.2-POF1	Includes Entity, Subsidiary, Division,	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
CC3.2-POF1	Operating Unit. and Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
CC3.2-POF2	Analyzes Internal and External Factors	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms useful admits a literature of the control of the contro	5	
CC3.2-POF2	Analyzes Internal and External Factors	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	10	
CC3.2-POF2	Analyzes Internal and External Factors	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications. Services and/or Data (TAASD).	5	
CC3.2-POF3	Involves Appropriate Levels of Management	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection 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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 conduct recurring assessments of risk that includes the	10	
CC3.2-POF3	Involves Appropriate Levels of Management	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Risk Assessment	RSK-04	likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications. Services and/or Data (TAASD).	10	
CC3.2-POF4	Estimates Significance of Risks Identified Estimates Significance of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions. Mechanisms exist to identify and assign a risk ranking to newly discovered security	5	
CC3.2-POF4 CC3.2-POF5	Risks Identified Determines How to	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	intersects with subset of	Risk Ranking Risk Management	RSK-05 RSK-01	vulnerabilities that is based on industry-recognized practices. Mechanisms exist to facilitate the implementation of strategic, operational and	5	
CC3.2-POF5	Respond to Risks Determines How to Respond to Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Program Risk Response	RSK-06.1	tactical risk management controls. Mechanisms exist to respond to findings from cybersecurity and data protection assessments, incidents and audits to ensure proper remediation has been	10	
CC3.2-POF6	Identifies Threats	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Identification	RSK-03	performed. Mechanisms exist to identify and document risks, both internal and external.	5	
CC3.2-POF6	Identifies Threats	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.2-POF6	Identifies Threats	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets,	5	
CC3.2-POF6	Identifies Threats	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Threat Intelligence Feeds Program	THR-01	Applications. Services and/or Data (TAASD). 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,	10	
CC3.2-POF6	Identifies Threats	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Indicators of Exposure (IOE)	THR-02	threat 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	
CC3.2-POF6	Identifies Threats	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
CC3.2-POF6	Identifies Threats	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.2-POF6 CC3.2-POF7	Identifies Threats Identifies Vulnerability of System Components	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	intersects with	Threat Analysis Supply Chain Risk Management (SCRM) Plan	THR-10 RSK-09	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats. Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting	5	
	Identifies Vulnerability of				Supply Chain Risk		selected mitigating actions and monitoring performance against those plans. Mechanisms exist to periodically assess supply chain risks associated with		
CC3.2-POF7	System Components Identifies Vulnerability of System Components	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	intersects with	Assessment Threat Intelligence Feeds Program	RSK-09.1 THR-01	Technology Assets, Applications and/or Services (TAAS). 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,	5	
CC3.2-POF7	Identifies Vulnerability of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Indicators of Exposure	THR-02	threat hunting, response and recovery activities. Mechanisms exist to develop Indicators of Exposure (IOE) to understand the	5	
CC3.2-POF7	System Components Identifies Vulnerability of System Components	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(IOE) Threat Intelligence Feeds Feeds	THR-03	obtential attack vectors that attackers could use to attack the oranization. Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
CC3.2-POF7	Identifies Vulnerability of System Components	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to	5	
CC3.2-POF7	Identifies Vulnerability of System Components	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	those risks and threats, as necessary. Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
CC3.2-POF7	Identifies Vulnerability of System Components Identifies Vulnerability of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.2-POF7	System Components	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Vulnerability Scanning	VPM-06	vulnerability scanning of systems and applications. Mechanisms exist to identify:	5	
CC3.2-POF8	Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Framing	RSK-01.1	(1) Assumptions affecting risk assessments, risk response and risk monitoring; 2) Constraints effecting risk assessments, risk response and risk monitoring; 3) The organizational risk tolerance; and 4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
CC3.2-POF8	Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
CC3.2-POF8	Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.2-POF8	Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unsuthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
CC3.2-POF8	Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.2-POF8	Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
	Parties		I	1	<u> </u>				



Secure Controls Framework (SCF) 13 of 4

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
CC3.2-POF8	Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high- value services.	(optional)	
CC3.2-POF8	Parties Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
CC3.2-POF8	Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPa) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to subcontractors.	5	
CC3.2-POF9	Parties Assesses the Significance of the Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TASSD).	5	
CC3.2-POF9	Assesses the Significance of the Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5	
CC3.2-POF9	Assesses the Significance of the Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high- value services.	5	
CC3.2-POF9	Assesses the Significance of the Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
CC3.2-POF9	Assesses the Significance of the Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.2-POF9	Assesses the Significance of the Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
CC3.2-POF9	Assesses the Significance of the Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
CC3.2-POF9	Assesses the Significance of the Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.3	COSO Principle 8	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	subset of	Threat Intelligence Feeds Program Indicators of Exposure	THR-01	Mechanisma exist to implement a threat infelligence 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. Mechanisma exist to develop influences of Exposure (IOE) to undestand the	10	
CC3.3	COSO Principle 8	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(IOE)	THR-02	potential stack vectors that attackers could use to attack the organization. Mechanisms exist to implement an insider threat program that includes a cross-	5	
CC3.3	COSO Principle 8 COSO Principle 8	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	intersects with	Insider Threat Program Third-Party Management	THR-04 TPM-01	discipline insider threat incident handling team. Mechanisms exist to facilitate the implementation of third-party management	5	
CC3.3	COSO Principle 8	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Acquisition Strategies,	TPM-03.1	controls. Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications	5	
CC3.3	COSO Principle 8	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Tools & Methods Third-Party Services	TPM-04	and/or Services (TAAS). Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
CC3.3	COSO Principle 8	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are	5	
CC3.3-POF1	Considers Various Types of Fraud	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Asset Governance	AST-01	consistent with and reflect organizational interests. Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
CC3.3-POF1	Considers Various Types of Fraud	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC3.3-POF1	Considers Various Types of Fraud Considers Various Types	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Threat Intelligence Feeds 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. Mechanisms exist to implement an insider threat program that includes a cross-	10	
CC3.3-POF1 CC3.3-POF2	of Fraud Assesses Incentives and	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	intersects with	Insider Threat Program Human Resources	THR-04 HRS-01	discipline insider threat incident handling team. Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC3.3-POF2 CC3.3-POF2	Pressures Assesses Incentives and Pressures	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security Management Threat Intelligence Feeds	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross- organization information-sharing capability that can influence the development of	10	
CC3.3-POF2	Assesses Incentives and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Program Insider Threat Program	THR-04	the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities. Mechanisms exist to implement an insider threat program that includes a cross-	10	
CC3.3-POF2	Pressures Assesses Opportunities	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources	HRS-01	discipline insider threat incident handling team. Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC3.3-POF3		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Security Management Threat Intelligence Feeds 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,	10	
CC3.3-POF3	Assesses Opportunities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Insider Threat Program	THR-04	threat hunting, response and recovery activities. Mechanisms exist to implement an insider threat program that includes a cross- disciplina incider threat incident handling team.	10	
CC3.3-POF4	Assesses Attitudes and Rationalizations	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management	HRS-01	discipline insider threat incident handling team. Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC3.3-POF4	Assesses Attitudes and Rationalizations	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Threat Intelligence Feeds 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	
CC3.3-POF4	Assesses Attitudes and Rationalizations	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.3-POF5	Considers the Risks Related to the Use of IT and Access to Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Threat Intelligence Feeds 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	
CC3.3-POF5	Considers the Risks Related to the Use of IT and Access to Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.4	COSO Principle 9	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	



cure Controls Framework (SCF) 14 of 4

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
CC3.4	COSO Principle 9	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	(optional) 5	
CC3.4	COSO Principle 9	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
	COSO Principle 9				Cybersecurity & Data Protection Representative		environment. Mechanisms exist to include a cybersecurity and/or data privacy representative in the configuration change control review process.		
CC3.4	COSO Principle 9	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	for Asset Lifecycle Changes Security Impact Analysis	CHG-02.3		5	
CC3.4	COSO Principle 9	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	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 and data	5	
CC3.4	COSO Principle 9	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection Portfolio Management	PRM-01	protection-related resource planning controls that define a viable plan for achieving cybersecurity and data protection objectives. Mechanisms exist to define business processes with consideration for cybersecurity	5	
					Business Process		and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other		
CC3.4	COSO Principle 9	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Definition	PRM-06	organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is	5	
					Third-Party Risk		obtained Mechanisms exist to conduct a risk assessment prior to the acquisition or		
CC3.4	COSO Principle 9	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Assessments & Approvals	TPM-04.1	outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS). Mechanisms exist to monitor, regularly review and assess External Service Providers	5	
CC3.4	COSO Principle 9	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Review of Third-Party Services	TPM-08	(ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	5	
CC3.4	COSO Principle 9	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5	
CC3.4-POF1	Assesses Changes in the External Environment Assesses Changes in the	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	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.	5	
CC3.4-POF1	External Environment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to conduct recurring assessments of risk that includes the	5	
CC3.4-POF1	Assesses Changes in the External Environment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Assessment	RSK-04	likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Apolications. Services and/or Data (TAASD).	5	
CC3.4-POF2	Assesses Changes in the Business Model	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Management Program	RSK-01	ADDITIONAL TIME TO A STATE OF THE ACT OF T	5	
CC3.4-POF2	Assesses Changes in the Business Model	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
CC3.4-POF2	Assesses Changes in the	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Power!	latara i iii	Distriction	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure,	5	
CC3.4-POF2	Business Model	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Assessment	HSK-04	disruption, modification or destruction of the organization's Technology Assets, Applications. Services and/or Data (TAASD).	5	
CC3.4-POF3	Assesses Changes in Leadership	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
CC3.4-POF3	Assesses Changes in	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Management	RSK-01	regular basis. Mechanisms exist to facilitate the implementation of strategic, operational and	5	
CC3.4-POF3	Leadership Assesses Changes in Leadership	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Program Risk Identification	RSK-03	tactical risk management controls. Mechanisms exist to identify and document risks, both internal and external.	5	
CC3.4-POF3	Assesses Changes in Leadership	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets,	5	
CC3.4-POF4	Assesses Changes in	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change Management	CHG-01	Applications. Services and/or Data (TAASD). Mechanisms exist to facilitate the implementation of a change management	5	
CC3.4-POF4	Systems and Technology Assesses Changes in Systems and Technology	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Program Configuration Change Control	CHG-02	program. Mechanisms exist to govern the technical configuration change control processes.	5	
CC3.4-POF4	Assesses Changes in Systems and Technology	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5	
CC3.4-POF4	Assesses Changes in Systems and Technology Assesses Changes in	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	subset of intersects with	Risk Management Program Risk Identification	RSK-01 RSK-03	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	
	Systems and Technology Assesses Changes in						Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure,		
CC3.4-POF4	Systems and Technology	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Assessment	RSK-04	disruption, modification or destruction of the organization's Technology Assets, Applications. Services and/or Data (TAASD).	5	
CC3.4-POF5	Assesses Changes in Vendor and Business Assesses Changes in	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.4-POF5	Vendor and Business Assesses Changes in	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to conduct recurring assessments of risk that includes the	5	
CC3.4-POF5	Vendor and Business Partner Relationships	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Assessment	RSK-04	likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Apolications. Services and/or Data (TAASD).	5	
CC3.4-POF5	Assesses Changes in Vendor and Business	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
	Partner Relationships Assesses Changes in						Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to		
CC3.4-POF5	Vendor and Business Partner Relationships	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Scope Review	TPM-05.5	ensure cybersecurity and data protection control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	
CC3.4-POF5	Assesses Changes in Vendor and Business	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity	5	
CC3.4-POF5	Partner Relationships Assesses Changes in Vendor and Business	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Managing Changes To Third-Party Services	TPM-10	and data protection controls. Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data	5	
	Partner Relationships Assesses Changes in				Third-Party Services Threat Intelligence Feeds		(TAASD) that are in scope by the third-party. Mechanisms exist to implement a threat intelligence program that includes a cross-		
CC3.4-POF6	Threats and Vulnerabilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Threat Intelligence Feeds Program	THR-01	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	
CC3.4-POF6	Assesses Changes in Threats and Vulnerabilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC3.4-POF6	Assesses Changes in Threats and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Vulnerability & Patch Management Program	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
CC3.4-POF6	Vulnerabilities Assesses Changes in Threats and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(VPMP) Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
CC3.4-POF6	Vulnerabilities Assesses Changes in Threats and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	
	Vulnerabilities Assesses Changes in				Vulnerability Exploitation		Mechanisms exist to identify, assess, prioritize and document the potential impact(s)		
CC3.4-POF6	Threats and Vulnerabilities Assesses Changes in	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Analysis	VPM-03.1	and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities. Mechanisms exist to detect vulnerabilities and configuration errors by routine	5	
CC3.4-POF6	Threats and Vulnerabilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Vulnerability Scanning	VPM-06	vulnerability scanning of systems and applications. Mechanisms exist to regularly review processes and documented procedures to	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements.	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection policies and standards.	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Audit Activities	CPL-04	Mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Measures of Performance	GOV-05	<u>business operations.</u> <u>Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.</u>	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Key Risk Indicators (KRIs)	GOV-05.2	of the cybersecurity and data protection program. Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Information Assurance (IA) Operations	IAO-01	cybersecurity and data protection program. Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.	5	
L		II.	1	1	(PA) Operations		p		



Secure Controls Framework (SCF) 15 of

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the opheracuity and data protection controls in Technology Assets, Applications and/or Services (RAST through Information Assurance Program (AP) activities to determine the extent to which the controls are implemented correctly, operating an intended and producing the desired outcome with respect to meeting expected requirements.	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Assessor Independence	IAO-02.1	Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct cybersecurity and data protection control assessments.	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	intersects with	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Saturbor, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Monitoring capabilities; (3) Monitoring capabilities; (5) Application security; (6) Application security; (7) Autorinopility management; (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Plan / Coordinate with Other Organizational	IAO-03.1	Intlantificial Intelligence and Automonous Technologies (AAT) Mechanisms exist to plan and coordinate Information Assurance Program (IAP) activities with affected stakeholders before conducting such activities in order to	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Entities Threat Analysis & Flaw Remediation During	IAO-04	reduce the potential impact on operations. Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Development Technical Verification	IAO-06	and remediate flaws during development. Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical cybersecurity	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Allocation of Resources	PRM-03	and data protection controls. Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection In Project Management	PRM-04	projects / initiatives. Mechanisms exist to assess cybersecurity and data protection 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	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Requirements Definition	PRM-05	meeting the requirements. Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	ISDICI. Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) information protection needs arising from the defined business processes and revises the processes as necessary, until an archievable set of protection needs is	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Management Program	RSK-01	obtained. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 or Technology Assets, Applications and/or Services (TAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection principles that addresses risk to organizational operations, assets, individuats, other organizations.	5	
CC4.1-POF1	Considers a Mix of Ongoing and Separate Evaluations	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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-P0F1	Considers a Mix of Ongoing and Separate Evaluations	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/inflagators consult with optersecurity and data protection personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability. (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	
CC4.1-POF2	Considers Rate of Change	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5	
CC4.1-POF2	Considers Rate of Change	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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. Mechanisms exist to implement an internal audit function that is capable of	5	
CC4.1-POF4	Uses Knowledgeable Personnel	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Internal Audit Function	CPL-02.1	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	intersects with	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Stattory, registancy and contractual compliance obligations; (2) Monitoring capabilities; (3) Mohile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Participations of the compliance of the contraction of the compliance of t	5	
CC4.1-POF5	Integrates With Business Processes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.	5	
CC4.1-POF8	Considers Different Types of Ongoing and Separate Evaluations	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity and data protection controls in Technology Assets, Applications and/or Services (TAAS) through information Assurance Program (AP) softwires to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
CC4.2	COSO Principle 17	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC4.2	COSO Principle 17	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection program.	5	
CC4.2	COSO Principle 17	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	



cure Controls Framework (SCF) 16 of 4

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
CC4.2	COSO Principle 17	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
CC4.2	COSO Principle 17	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
CC4.2	COSO Principle 17	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Remediation	RSK-06	eliminate known vulnerabilities. Mechanisms exist to remediate risks to an acceptable level.	5	
CC4.2	COSO Principle 17	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to	5	
CC4.2	COSO Principle 17	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Deficiency Remediation	TPM-09	production. Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
CC4.2	COSO Principle 17	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
CC4.2	COSO Principle 17	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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. Mechanisms exist to coordinate cybersecurity, data protection and business	5	
CC4.2-POF1	Assesses Results	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	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	
CC4.2-POF1	Assesses Results	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection program.	5	
CC4.2-POF1	Assesses Results	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance. Mechanisms exist to document and review instances of non-compliance with	5	
CC4.2-POF1	Assesses Results	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Non-Compliance Oversight Cybersecurity & Data	CPL-01.1	statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to provide a cybersecurity and data protection controls oversight	5	
CC4.2-POF1	Assesses Results	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection Controls Oversight	CPL-02	function that reports to the organization's executive leadership. Mechanisms exist to compel data and/or process owners to assess if required	5	
CC4.2-POF1	Assesses Results	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Assess Controls	GOV-15.3	cybersecurity and data protection controls for each system, application and/or service under their control are implemented correctly and are operating as intended.	5	
CC4.2-POF2	Communicates Deficiencies	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC4.2-POF2	Communicates Deficiencies	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection program.	5	
CC4.2-POF2	Communicates Deficiencies	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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-POF2	Communicates Deficiencies	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	5	
CC4.2-POF3	Monitors Corrective Action	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	5	
CC4.2-POF3	Monitors Corrective Action	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC4.2-POF3	Monitors Corrective Action	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
CC5.1	COSO Principle 10	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compet data and/or process owners to operationalize cybersecurity and data protection practices for each system, application and/or service under their control.	5	
CC5.1	COSO Principle 10	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity and data protection controls for each system, application and/or service under their control.	5	
CC5.1	COSO Principle 10	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Implement Controls	GOV-15.2	service under their control.	5	
GC5.1	COSO Principle 10	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion. Mechanisms exist to identify and document Standardized Operating Procedures	5	
CC5.1	COSO Principle 10	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	(SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
CC5.1	COSO Principle 10	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security Concept Of Operations (CONOPS)	OPS-02	Mechanisms exist to develop a security Concept of Operations (CONPS), 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	
							Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines:		
CC5.1	COSO Principle 10	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	The resulting risk to organizational operations, assets, individuals and other organizations; and Information protection needs arising from the defined business processes and	5	
					Risk Management		revises the processes as necessary, until an achievable set of protection needs is 		



Secure Controls Framework (SCF) 17 of 40

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CC5.2	COSO Principle 11	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection In Project Management	PRM-04	Mechanisms exist to assess cybersecurity and data protection 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	5	
CC5.2	COSO Principle 11	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Requirements Definition	PRM-05	meeting the requirements. Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle ISDLCI.	5	
CC5.2	COSO Principle 11	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and organizations are designed to the organization of the org	5	
CC5.2	COSO Principle 11	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Development Life Cycle (SDLC)	PRM-07	Ahtainard Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled	5	
CC5.2	COSO Principle 11	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management Business Impact Analysis (BIA)	RSK-08	through formal change control procedures. Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	5	
CC5.2	COSO Principle 11	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
CC5.2	COSO Principle 11	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized ophersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS), Mechanisms exist to facilitate the implementation of tailored development and	5	
CC5.2	COSO Principle 11	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Technology Development & Acquisition	TDA-01	acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
CC5.2	COSO Principle 11	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
CC5.2-POF1	Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	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	
CC5.2-POF2	Establishes Relevant Technology Infrastructure Control Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Control Applicability Boundary Graphical Representation	AST-04.2	Mechanisms exist to ensure control applicability is appropriately-determined for Technology Assets, Applications and/or Services (TAAS) and third parties by graphically representing applicable boundaries.	5	
CC5.2-POF2	Establishes Relevant	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
CC5.2-POF3	Establishes Relevant Security Management Process Controls	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
CC5.2-POF3	Establishes Relevant Security Management Process Controls Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC5.2-POF4	Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC5.3	COSO Principle 12	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	
CC5.3	COSO Principle 12	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection 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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC5.3	COSO Principle 12	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Personnel Security	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third- party cybersecurity and data protection roles and responsibilities. Mechanisms exist to identify and document Standardized Operating Procedures	5	
CC5.3	COSO Principle 12 Establishes Policies and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	(SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
CC5.3-POF1	Procedures to Support Deployment of Management's Directives	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	
CC5.3-POF1	Establishes Policies and Procedures to Support Deployment of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business As Usual (BAU) Secure Practices	GOV-14	Mechanisms exist to incorporate cybersecurity and data protection principles into Business As Usual (BAU) practices through executive leadership involvement.	5	
CC5.3-POF2	Executing Policies and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	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 enterorise-wide cybersecurity and data protection program. Mechanisms exist to enforce an accountability structure so that appropriate teams	5	
CC5.3-POF2	Establishes Responsibility and Accountability for Executing Policies and Procedures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1	and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	
CC5.3-POF2	Establishes Responsibility and Accountability for Executing Policies and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
CC5.3-POF3	Performs in a Timely Manner	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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-POF3	Performs in a Timely Manner	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 coals of the process area.	5	
CC5.3-POF4	Takes Corrective Action	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Remediation Vulnerability Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and	5	
CC5.3-POF4	Takes Corrective Action	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Process Al & Autonomous	VPM-02	remediated. Mechanisms exist to ensure Artificial Intelligence (Al) and Autonomous Technologies (AAT-related operator and practitioner proficiency requirements for Artificial	5	
CC5.3-POF5	Performs Using Competent Personnel	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Technologies Stakeholder Competencies Competency	AAT-13.1	Intelligence (AI) and Autonomous Technologies (AAT) are defined, assessed and documented. Mechanisms exist to ensure that all security-related positions are staffed by	5	
CC5.3-POF5	Performs Using Competent Personnel	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Requirements for Security- Related Positions	HRS-03.2	qualified individuals who have the necessary skill set. Mechanisms exist to review the cybersecurity and data protection program,	5	
CC5.3-POF6	Reassesses Policies and Procedures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	10	
CC5.3-POF6	Reassesses Policies and Procedures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Measures of Performance Use of Cryptographic	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance. Mechanisms exist to facilitate the implementation of cryptographic protections	5	
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Controls Transmission	CRY-01	controls using known public standards and trusted cryptographic technologies. Cryptographic mechanisms exist to protect the confidentiality of data being	5	
CC6.1	N/A N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	intersects with	Confidentiality Encrypting Data At Rest	CRY-03	transmitted. Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Public Key Infrastructure	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	
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(PKI) Cryptographic Key	CRY-09	Immatructure or obtain PAI services from a reputable PAI service provider. Mechanisms exist to facilitate cryptographic key management controls to protect the	5	
GG8.1	NIA	STATIONAL ASSETA STATUSES CAREINA (15C) FOR Specific control wording.	runctionat	ancer sects with	Management	UNT-09	confidentiality, integrity and availability of keys.		1



cure Controls Framework (SCF) 18 of 4

Part	FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
Part	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Symmetric Keys	CRY-09.1	cryptographic keys using Federal Information Processing Standards (FIPS)-	5	
March Marc	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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)-	5	
Part	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IAC-01		5	
1985 1985	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identification &	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and	5	
March Marc						Organizational Users Identification &		users. Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and		
Mathematical Math	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IAC-03		5	
Math	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authentication for Devices	IAC-04	Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.	5	
Property	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authentication for Third- Party Technology Assets, Applications and/or	IAC-05		5	
Mail	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Role-Based Access	IAC-08	Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals	5	
March Marc	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(User Names)	IAC-09	Assets, Applications and/or Services (TAAS).	5	
Second Column Property Prop	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IAC-09.1	consumer users and administrators.	5	
Section Sect	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IAC-10	(1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the	5	
March Marc	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account	5	
March Marc	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group,	5	
March Marc	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IAC-16	Technology Assets, Applications and/or Services (TAAS).	5	
1901 180	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Access Enforcement	IAC-20	to the principle of "least privilege."	5	
Col. Section	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Least Privilege	IAC-21	access to processes necessary to accomplish assigned tasks in accordance with	5	
Col.	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the	5	
Col.	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		NET-03	Mechanisms exist to monitor and control communications at the external network	5	
Second S	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Connections	NET-03.1		5	
Col. Mail	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Access Control Lists	NET-04	configurations to restrict connections between untrusted networks and internal	5	
Cold Max	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	intersects with	External System	NFT-05.1	Mechanisms exist to prohibit the direct connection of a sensitive system to an	5	
								device. Mechanisms exist to ensure network architecture utilizes network segmentation to	-	
Col. 1971	CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		NE1-06	network resources. Mechanisms exist to implement security management subnets to isolate security	5	
Col. Folia Interface colleges Col.	CC6.1		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		NET-06.1	implementing separate subnetworks with managed interfaces to other components of the system.	5	
Section Continued Section Continued Continued Section Continued Contin	CC6.1-POF1		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Asset Governance	AST-01	and manage asset management controls.	10	
Section 1 Sectio	CC6.1-POF1	the Inventory of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Asset Inventories	AST-02	Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software producth, including business justification details; (3) is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability, and	5	
DOS. 1970 - 19 No houtbury of control services (Control (TC)) for specific control wording. OS. 1970 - 197	CC6.1-POF1	the Inventory of Information Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Asset Scope Classification	AST-04.1	applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5	
COST 1-POTO PARTICIPATION APPRIEST AND PARTICIPATION SERVICES CHARGE POTO PARTICIPATION AND PARTICIPAT	CC6.1-POF1	the Inventory of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		DCH-02		5	
Asserting Septiment of the Control of Part Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921) for specific control wording, Punctional. COS. 1-POPS Asserting Regulation Services (China (1921)	CC6.1-POF2	Assesses New	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Information Assurance	IAO-01	protection assessment and authorization controls.	10	
Assesses New Architectures COS. 1-POTS Assesses New Architectures Assesses New Architectures Assesses New Architectures Assesses New Architectures COS. 1-POTS Assesses Lugical Access Coversional AICPNA Trust Services Critical (SCC) for specific control wording COS. 1-POTS Assesses New Architectures COS. 1-POTS Assesses New Architectures COS. 1-POTS	CC6.1-POF2		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Assessments	IAO-02	in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing	5	
Accessed New Accessed New Accessed New Accessed Annual Control Page of the Control Newsoring Plant Con	CC6.1-POF2	PADDODDOD I TOTT	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		SEA-01	cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
Col. 1-POT3 Restricts Lagical Access Dominioal AICPA's Trust Services Criteria (TSC) for specific control wording. Functional sterenects with Authoriticate, Authorities and Audit (PAA) Moderations and to servicing yourn the use of Authoriticate, Authorities and Audit (PAA) Moderations and three houses of present to service the presentation of selectification and access and three houses by an Exercise Vision and Audit (PAA) Moderations and three houses by an Exercise Vision and Audit (PAA) Moderations and three houses by an Exercise Vision and Audit (PAA) Moderations and three houses by an Exercise Vision and Audit (PAA) Moderations and three houses by an Exercise Vision and Audit (PAA) Moderations and three houses by an Exercise Vision and Audit (PAA) Moderations and three houses by an Exercise Vision and Audit (PAA) Moderations and three houses by an Exercise Vision and Audit (PAA) Moderations and three houses and processes accing to the hold for organizational data of Audit (PAA) and Audit (PAA) Moderations and processes accing to the hold for organizational data of Audit (PAA) Moderations and processes accing to the hold of Audit (PAA) Moderations and processes accing to the hold for organizational data of Audit (PAA) Moderations and processes accing to the hold of Audit (PAA) Moderations and processes accing to the hold of Audit (PAA) Moderations and processes accing to the hold of Audit (PAA) Moderations and processes accing to the hold of Audit (PAA) Moderations and processes accing to the hold of Audit (PAA) Moderations and processes accing to the hold of Audit (PAA) Moderations and processes accing to the hold of Audit (PAA) Moderations and processes accing to the hold of Audit (PAA) Moderations and processes accing to the hold of Audit (PAA) Moderations and processes accing to the hold of Audit (PAA) Moderations and processes accing to the hold of Audit (PAA) Moderations and processes accing to the hold of Audit (PAA) Moderations and process	CC6.1-POF2		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		SEA-02	recognized leading practices, with consideration for cybersecurity and data protection principles that addresses risk to organizational operations, assets,	5	
Pestricts Logical Access Constrol ACPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Authentication for Authentication for Authentication for Authentication for Authentication for Notice Services Criteria (TSC) for specific control wording. Functional intersects with Authentication for Authentication for Notice Services Criteria (TSC) for specific control wording. Functional intersects with Authentication for Notice Services Criteria (TSC) for specific control wording. Functional intersects with Authentication for Notice Services Criteria (TSC) for specific control wording. Functional intersects with Authentication for Notice Services Criteria (TSC) for specific control wording. Functional intersects with Authentication for Notice Services Criteria (TSC) for specific control wording. Functional intersects with Authentication for Notice Services Criteria (TSC) for specific control wording. Functional intersects with Authentication for Notice Services Criteria (TSC) for specific control wording. Functional intersects with Authentication for Notice Services Criteria (TSC) for specific control wording. Functional intersects with Authenticates Users CC6.1-POF4 Identifies and Authenticates Users Ownerload AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Authenticates Users CC6.1-POF4 Identifies and Authenticates Users Ownerload AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Authenticates Users CC6.1-POF4 Identifies and Authenticates Users Ownerload AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Authenticates Users and Audit (AIA) applications and Audit (AIA) policional survey identity and centrally Authenticate, Authorica and Audit (AIA) policional survey identity and centrally Authenticate, Authorica and Audit (AIA) policional survey identity and centrally Authenticate, Authorica and Audit (AIA) policional survey id	CC6.1-POF3	Restricts Logical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of		IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
Restricts Logical Access Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Authentication of Authentication of Non-Organizational users and processes acting on behalf of organizational users and processes acting on behalf of organizational users. Authentication for Non-Organizational users and processes acting on behalf of organizational users. Authentication for Non-Organizational users and processes acting on behalf of organizational users. Authentication for Non-Organizational users and processes acting on behalf of organizational users. Authentication for Non-Organizational users and processes acting on behalf of organizational users. Authentication for Non-Organizational users and processes that provide services to the organization. S Segmentation Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with intersects with Authentication for Non-Organizational users and processes acting on behalf of organizational users. Authentication & Authentication for Non-Organizational users and processes acting on behalf of organizational users. CC6.1-POF4 Alternities and Authenticates Users Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Authentication for Non-Organizational users and processes acting on behalf of organizational users. Authentication & Authentication & Authentication for Non-Organizational users and processes acting on behalf of organizational users. CC6.1-POF4 Authenticates Users Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Control wording. Functional intersects with Control wording. Functional inters	CC6.1-POF3	Restricts Logical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IAC-01.2	(AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
Restricts Logical Access Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC8.1-PDF3 Restricts Logical Access Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Authentication 8 Authentication 16	CC6.1-POF3	Restricts Logical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authentication for	IAC-02	Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
Restricts Logical Access Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Authentication for Devices Authentication for Devices Authentication for Devices Authentication for Devices Authenticates Authorize and Authenticates Authorize and Authenticates Authorize and Authenticates Authorize and Authorize and Authorize and Authorize and Authorizes and Authenticates Users	CC6.1-POF3	Restricts Logical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authentication for Non-	IAC-03	Audit (AAA) third-party users and processes that provide services to the organization.	5	
Constitution Cons	CC6.1-POF3	Restricts Logical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IAC-04	Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.	5	
CC8.1-POF4 Identifies and Authenticates Users CC8.1-POF4 Identifies and Authenticates Users CC8.1-POF4 Identifies and Authenticates Users CC8.1-POF5 Considers Network Segmentation (macrosegmentation) CC8.1-POF5 CR.1-POF5 CR.1-POF5 Segmentation (macrosegmentation) CC8.1-POF5 CR.1-POF5 CR.1-POF5 Segmentation (macrosegmentation) CC8.1-POF5 CR.1-POF5 Segmentation (macrosegmentation) CC8.1-POF5 Segmentation (macrosegment	CC6.1-POF4		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	and Audit (AAA)	IAC-01.2	(AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
Constitution Cons	CC6.1-POF4		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authentication for	IAC-02	Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
CS.1-POFS Segmentation processes and segmentation processes are secure and segmentation processes are secure and segmentati	CC6.1-POF4		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authentication for Non-	IAC-03		5	
CC6.1-POFS	CC6.1-POF5	Segmentation	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cloud Services	CLD-01	ensure cloud instances are secure and in-line with industry practices.	5	
Considers Network Cos.1-POF5 Segmentation Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with (NSC) NET-01 implementation of Network Security Controls (NSC). 5	CC6.1-POF5	Segmentation	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		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	5	
	CC6.1-POF5	Segmentation	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the	5	



Secure Controls Framework (SCF) 19 of 4

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CC6.1-POF5	Considers Network Segmentation (macrosegementation)	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Zero Trust Architecture (ZTA)	NET-01.1	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized.	5	
CC6.1-POF5	Considers Network Segmentation	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC6.1-POF5	(macrosegementation) Considers Network Segmentation	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC6.1-POF6	Manages Points of Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Flow Enforcement – Access Control Lists	NET-04	Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal	5	
CC6.1-POF6	Manages Points of Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(ACLs) Managed Access Control Points	NET-14.3	systems. Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	5	
CC6.1-POF7	Restricts Access to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure basetine configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	
CC6.1-POF7	Restricts Access to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Least Functionality	CFG-03	consistent with industry-accepted system hardening 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	Information Assets Restricts Access to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identity & Access	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
CC6.1-POF7	Information Assets Restricts Access to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management (IAM) 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	5	
CC6.1-POF8	Information Assets Manages Identification	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Identity & Access	IAC-01	organizational business functions. Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
CC6.1-POF8	and Authentication Manages Identification	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management (IAM) Identification & Authentication for	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational	5	
CC6.1-POF8	and Authentication Manages Identification	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Organizational Users Identification &	IAC-04	Weehanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional	5	
CC6.1-POF8	and Authentication	Download AICPA'S Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authentication for Devices Identification &	IAC-04	authentication that is cryptographically- based and replay resistant. Mechanisms exist to identify and authenticate third-party Technology Assets,	•	
CC6.1-POF8	Manages Identification and Authentication	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authentication for Third- Party Technology Assets, Applications and/or Services (TAAS)	IAC-05	Applications and/or Services (TAAS). Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement	5	
CC6.1-POF9	Manages Credentials for Infrastructure and Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Asset Governance	AST-01	and manage asset management controls.	5	
CC6.1-POF9	Manages Credentials for Infrastructure and Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
CC6.1-POF9	Manages Credentials for Infrastructure and Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.	5	
CC6.1-POF9	Manages Credentials for Infrastructure and Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
CC6.1-POF10	Uses Encryption to Protect Data	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC6.1-POF10	Uses Encryption to Protect Data	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
CC6.1-POF10	Uses Encryption to Protect Data Uses Encryption to Protect	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	intersects with	Transmission Integrity Encrypting Data At Rest	CRY-04 CRY-05	Cryptographic mechanisms exist to protect the integrity of data being transmitted. Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
CC6.1-POF10	Data Uses Encryption to Protect	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Public Key Infrastructure	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	
CC6.1-POF10	Data Uses Encryption to Protect	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(PKI) Cryptographic Key	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the	5	
CC6.1-POF10	Data Uses Encryption to Protect Data	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management Symmetric Keys	CRY-09.1	confidentiality. integrity and availability of keys. Mechanisms exist to facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS)-	5	
CC6.1-POF10	Uses Encryption to Protect Data	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Asymmetric Keys	CRY-09.2	compliant key 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	5	
CC6.1-POF11	Protects Cryptographic Keys	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Use of Cryptographic Controls	CRY-01	kev. Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
CC6.1-POF11	Protects Cryptographic Keys	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC6.1-POF11	Protects Cryptographic Keys	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC6.1-POF11	Protects Cryptographic Keys	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Asymmetric Keys	CRY-09.2	compliant key management recinionly 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	5	
CC6.1-POF11	Protects Cryptographic	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cryptographic Key Loss or Change	CRY-09.3	key. Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5	
CC6.1-POF11	Protects Cryptographic	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Control & Distribution of	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and	5	
CC6.1-POF12	Restricts Access to and Use of Confidential	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cryptographic Keys Role-Based Access	IAC-08	processes. Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals	5	
CC6.1-POF12	Information for Identified Restricts Access to and Use of Confidential Information for Identified	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Control (RBAC) Access To Sensitive / Regulated Data	IAC-20.1	assigned specific roles with legitimate business needs. Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.	5	
CC6.1-POF12	Purposes Restricts Access to and Use of Confidential Information for Identified	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	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	Purposes Restricts Access to and the Use of Personal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Role-Based Access	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals	5	
CC6.1-POF13	Information Restricts Access to and the Use of Personal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Control (RBAC) Access To Sensitive / Regulated Data	IAC-20.1	assigned specific roles with legitimate business needs. Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.	5	
CC6.1-POF13	Information Restricts Access to and the Use of Personal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
CC6.1-POF13	Information Restricts Access to and the Use of Personal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security of Personal Data (PD)	PRI-01.6	organizational business functions. Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the	5	
CC6.1-POF13	Information Restricts Access to and the Use of Personal Information	Downtoad AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	confidentiality and integrity of the PD. Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes, and (2) Authorizes the use of PD when such information is required for internal testing.	5	
CC6.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Provisioning & De- Provisioning	IAC-07	training and research Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
CC6.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
CC6.2-POF1	Creates Access Credentials to Protected	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Provisioning & De-	IAC-07	unnecessarv privileges, as necessarv. Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
CC6.2-PUF1	Information Assets	DOWNLOOD ALGEN S TRUST Services Gitteria (LSG) for specific control wording.	runctional	intersects with	Provisioning	IAC-07		•	



Secure Controls Framework (SCF) 20 of 4

Column	FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
								Mechanisms exist to revoke user access rights following changes in personnel roles	(optional)	
Second Column	CC6.2-POF1		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change of Roles & Duties	IAC-07.1		5	
	CC6.2-POF1	Credentials to Protected	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IAC-28.1		5	
	CC6.2-POF2	Reviews Validity of Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change of Roles & Duties	IAC-07.1		5	
March Marc	CC6.2-POF2	Reviews Validity of Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-	5	
Transport	CC6.2-POF2	Reviews Validity of Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	System Account Reviews	IAC-15.7	Mechanisms exist to review all system accounts and disable any account that	5	
Description Company	CC6 2 BOE2			Eupstional	intercepts with	Periodic Review of	IAC 17	Mechanisms exist to periodically-review the privileges assigned to individuals and	E	
Column		Prevents the Use of						unnecessary privileges, as necessary. Mechanisms exist to adjust logical and physical access authorizations to Technology		
Part		Longer Valid						reassignment or transfer, in a timely manner.	_	
March Marc		Prevents the Use of						Mechanisms exist to utilize a formal user registration and de-registration process	5	
March Marc		Longer Valid Prevents the Use of		runctional			IAC-U/		•	
Control Cont	CC6.2-POF3	Longer Valid	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IAC-15.7	·	5	
Company Comp	CC6.2-POF3	Credentials When No	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IAC-17	service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	
1975 1975	CC6.3		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Control (RBAC)	IAC-08	Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals	10	
Control Cont	CC6.3-POF1	Access to Protected	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IAC-07	that governs the assignment of access rights.	5	
Second Control Second Control Se	CC6.3-POF1	Access to Protected Information Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change of Roles & Duties	IAC-07.1	and duties, if no longer necessary or permitted.	5	
	CC6.3-POF1	Access to Protected	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IAC-28.1		5	
Control Cont	CC6.3-POF2	Removes Access to Protected Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IAC-07	that governs the assignment of access rights.	5	
Control Cont	CC6.3-POF2	Protected Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change of Roles & Duties	IAC-07.1		5	
Processing	CC6.3-POF3	Uses Access Control	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal		IAC-08	Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals	10	
Big Section Big Sectio	CC6.3-POF4		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal		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	10	
Column Part Column Col	CC6.4		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PES-01	Mechanisms exist to facilitate the operation of physical and environmental	5	
Cold 18	CC6.4	NIA	Doubland ALCRA's Trust Sandage Criteria (TSC) for appoint a central wording	Eupstional	intercepts with		DES 02			
Cold 18								facility officially designated as publicly accessible).		
COS. 4 POINT Consider Michigan	CC6.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PES-02.1		5	
CCEL-POTO Demonstrations of the control of the cont	CC6.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical Access Control	PES-03	for all physical access points (including designated entry/exit points) to facilities	5	
COLLAPOTI CHARGE PROJECT CONTROL CONTR	CC6.4-POF1		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PES-01		5	
COLA-FOTO Project Access Project Acc	CC6.4-POF1		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PES-02	with authorized access to organizational facilities (except for those areas within the	5	
COLA POT Notice of Ministry Physical Access Device (ACPAN Trace Services College (CDA) Project (ACPAN Trace Services College (CD	CC6.4-POF1		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities	5	
CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Renove Physical Access Described ACPA's Trust Services Crisis (RCS) to specific control useding. CGL 4PG7 Reno	CC6.4-POF1		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical Access Control	PES-03	for all physical access points (including designated entry/exit points) to facilities	5	
CCL 4-PCP2 Acrossor Physical Access Construction Control Contr		· ·				Physical & Environmental				
The Code A POTO Remons Physical Access to Deveload ACPA's Trust Services Chiese (TSC) for specific control working. COS. 4 POTO Remons Physical Access to Deveload ACPA's Trust Services Chiese (TSC) for specific control working. Procticoal statements with the control physical access to the control access and the contro	CC6.4-POF2	Removes Physical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PES-01		5	
CCS.4 POY2 Remove Physical Access Download ACPVs Trust Services Critical PSC) for specific control wording. CCS.4 POY2 Remove Physical Access Download ACPVs Trust Services Critical PSC) for specific control wording. Proceedings of the process o	CC6.4-POF2	Removes Physical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PES-06.6	surrendered before visitors leave the facility or are deactivated at a pre-determined time/date of expiration.	5	
CCS. 4 PCP2 Remove Physical Access Control RPDN Trust Services Citizen (TSC) for specific control wording. CCS. 4 PCP3 Remove Physical Access Control Physical Devices AICPN Trust Services Citizen (TSC) for specific control wording. CCS. 4 PCP3 Remove Physical Access Control Physical Devices AICPN Trust Services Citizen (TSC) for specific control wording. CCS. 4 PCP3 Remove Physical Access Control Physical Devices AICPN Trust Services Citizen (TSC) for specific control wording. CCS. 4 PCP3 Remove Physical Access Control Physical Physical Access Control Physical Physical Access Control Physical Physical Access Control Ph	CC6.4-POF2	Removes Physical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authorizations	PES-02	with authorized access to organizational facilities (except for those areas within the	5	
Recover Physical Access Control of physical Access Control of physical Access Control of physical Access Control of physical access control physical degraded and physical degraded and physical deciding (Thors possible of physical access Control of physical access	CC6.4-POF2	Removes Physical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PES-02.1	based on the position or role of the individual.	5	
CC6.4-PGT Mechani Projection Mechanism and the protection Mechanism and the protection Section S	CC6.4-POF2	Removes Physical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical Access Control	PES-03	for all physical access points (including designated entry/exit points) to facilities	5	
CC6.4 PCF4 RoMers Physical Access Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Psycial Access Logs Romers Physical Access Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Psycial Access Logs Romers Physical Access Logs Romers Physical Access Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Psycial Access Logs Romers Physical Access Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Romers Physical Access Logs Romers Rome	CC6.4-POF3		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Return of Assets	AST-10	organizational assets in their possession upon termination of employment, contract	5	
CCB.4 POFA Reviews Physicial Access N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional CCB.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional	CC6.4-POF3	Recovers Physical	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Asset Collection	HRS-09.1	Mechanisms exist to retrieve organization-owned assets upon termination of an	5	
Source Proposed And Park Trust Services Criteria (TSC) for specific control wording. CC6.5 NA Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Physical Media Singuistation of the Service Singuistation of Singuistation Singuistation of Singuistation Singuistation of Singuistatio	CC6.4-POF4		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	5	
Devision ACPA's Trust Services Criteria (TSC) for specific control wording. CC6.5 N/A Download ACPA's Trust Services Criteria (TSC) for specific control wording. CC6.5 N/A Download ACPA's Trust Services Criteria (TSC) for specific control wording. CC6.5 N/A Download ACPA's Trust Services Criteria (TSC) for specific control wording. CC6.5 N/A Download ACPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Destruction or Removed to the components. CC6.5 N/A Download ACPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Destruction or Removed to the components. Functional intersects with Destruction or Removed to the components of the components. CC6.5 N/A Download ACPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Destruction or Removed to the components of the components of the components of the components of the components. CC6.5 N/A Download ACPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Destruction or Removed to the components of t	CC6.4-POF4	Reviews Physical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Access	PES-05	physical security incidents.	10	
Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Prunctional Intersects with Prunctional Intersects with Prunctional Intersects with Prunctional Intersects with System Media Sanitization DCH-09 Mechanisms exist to sacurely dispose of media when it is no longer required, using from proper formation being somewhere a cost to sanitize system media with the strength and integrity formation procedures. DCH-09 Mechanisms exist to sanitize system media with the strength and integrity formation being a disposal returns and integrity of the information prior to disposal returns and integrity deposition or sensitivity of the information prior to disposal returns and or prevariational control revised for reuse. DCR-5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Intersects with Intersects with Personal Data (PD) Retention & Disposal DCH-21 Mechanisms exist to: (1) Retain Personal Data (PD) Retention & Disposal DCH-21 Mechanisms exist to: (1) Retain Personal Data (PD) Retention & Disposal DCH-22 Mechanisms exist to: (1) Retain Personal Data (PD) Retention & Disposal DCH-23 Mechanisms exist to: (1) Retain Personal Data (PD) Retention & Disposal DCH-25 Mechanisms exist to: (1) Retain Personal Data (PD) Retention & Disposal DCH-26 Mechanisms exist to: (1) Retain Personal Data (PD) Retention & Disposal DCH-27 Mechanisms exist to: (1) Retain Personal Data (PD) Retention & Disposal DCH-27 Mechanisms exist to: (1) Retain Personal Data (PD) Retention & Disposal DCH-27 Mechanisms exist to: (1) Retain Personal Data (PD) Retention & Disposal DCH-27 Mechanisms exist to: (1) Retain Personal Data (PD) Retention & Disposal DCH-27 Mechanisms exist to: (1) Retain Personal Data (PD) Retention & Disposal (2) Dispose of, destroy, a rease, and/or an organization-defined tenine persona	CC6.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of		DCH-01		10	
CC6.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Physical Media Disposal DCH-09 trust Services Criteria (TSC) for specific control wording. Functional intersects with process of the services Criteria (TSC) for specific control wording. Functional intersects with Information Disposal DCH-09 commonsurate with the classification or sensitivity of the information prior to 5 commonsurate with the classification or release for resease. Mechanisms exist to securely dispose of, destroy or ense information. DCH-09 commonsurate with the classification or sensitivity of the information prior to 5 commonsurate with the classification or release for resease. Mechanisms exist to securely dispose of, destroy or ense information. DCH-01 Trust Services Criteria (TSC) for specific control wording. Functional intersects with process of the services Criteria (TSC) for specific control wording. Functional intersects with process of the services Criteria (TSC) for specific control wording. Functional intersects with process of the services Criteria (TSC) for specific control wording. Functional intersects with process of the services Criteria (TSC) for specific control wording. Functional intersects with process of the services Criteria (TSC) for specific control wording. Functional intersects with process of the services Criteria (TSC) for specific control wording. Functional intersects with process of the services Criteria (TSC) for specific control wording. Functional intersects with process of the services Criteria (TSC) for specific control wording. Functional intersects with process of the services Criteria (TSC) for specific control wording. Functional intersects with process of the services Criteria (TSC) for specific control wording. Functional intersects with process of the services Criteria (TSC) for specific control wording. Functional intersects with process of the services Criteria (TSC) for specific control wording. Functional interse	CC6.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Destruction or Re-Use of	AST-09	using organization-defined techniques and methods to prevent information being recovered from these components.	5	
CC6.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with pownload AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Information Disposal DCH-21 Mechanisms exist to securely dispose of, destroy or erase information. Mechanisms exist to securely dispose of, destroy or erase information. Mechanisms exist to securely dispose of, destroy or erase information. Mechanisms exist to provide a Michanisms exist to securely dispose of, destroy or erase information. Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfit the purpose) player period to fulfit the purpose player period to fulfit the purpose) player period to fulfit the purpose player period to fulfit the	CC6.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical Media Disposal	DCH-08	formal procedures.	5	
CC6.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Disposal (PPI-50 AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Disposal (PPI-50 AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Disposal (PPI-50 AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Disposal (PPI-50 AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Disposal (PPI-50 AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Disposal (PPI-50 AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Disposal (PPI-50 AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Disposal (PPI-50 AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Disposal (PPI-50 AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Disposal (PPI-50 AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Disposal (PPI-50 AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Disposal (PPI-50 AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Disposal (PPI-50 AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Disposal (PPI-50 AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Disposal (PPI-50 AICPA's Trust Services Criteria (TSC) for speci	CC6.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	System Media Sanitization	DCH-09	commensurate with the classification or sensitivity of the information prior to	5	
CC6.5 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Personal Data (PD) Retention a Disposal PRIOR Trust Services Criteria (TSC) for specific control wording. Functional intersects with Personal Data (PD) Retention a Disposal PRIOR Trust Services Criteria (TSC) for specific control wording. N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. N/A	CC6.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Information Disposal	DCH-21		5	
Removes Data and Software for Disposal Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Destruction or Re-Use of Equipment Secure Disposal, AST-09 Equipment Secure Disposal AST-09 Removes Data and Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Destruction or Re-Use of Equipment Secure Disposal, AST-09 Equipment Secure Disposal, AST-09 Equipment Secure Disposal, Disposal Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Destruction or Re-Use of Disposal, Disposal Disposal, Disposal, Disposal Disposal, Disposal Disposal, Disposal Disposal, Disposal Disposal, Disposal Disposal, Disposa						Retention & Disposal		(1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purposely) identified in the notice or a required by Iam? (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage, and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).		
CC6.5-POF2 Removes Data and Software for Disposal Software for Disposal Pownload AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Destruction of Re-Use of Equipment. Personal Pownload AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Destruction of Re-Use of Equipment. Personal Pownload AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Destruction of Re-Use of Equipment. Provided Marks Disposal Pownload AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Destruction of Re-Use of Equipment. Provided Marks Disposal Pownload AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Destruction of Re-Use of Equipment. Provided Marks Disposal provided and prov	CC6.5-POF1		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	N/A	N/A		N/A		5	Removed from TSC 2017
Removes Data and Download AICPA's Trust Sandree Criteria (TSC) for enertify working Europinal intersects with Physical Marks Disposed Drugs formal procedures.	CC6.5-POF2		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Destruction or Re-Use of	AST-09	using organization-defined techniques and methods to prevent information being recovered from these components.	5	
Software for Disposal Software for Disposal	CC6.5-POF2		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical Media Disposal	DCH-08		5	



Secure Controls Framework (SCF) 21 of 40

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
CC6.5-POF2	Removes Data and Software for Disposal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
CC6.5-POF2	Removes Data and Software for Disposal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5	
CC6.5-POF2	Removes Data and Software for Disposal	Download ACPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fuffill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
CC6.6	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
CC6.6	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
CC6.6	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Network Security Controls (NSC)	NET-01	(ESP). Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
CC6.6	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	5	
CC6.6	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC6.6	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications and/or Services [TAAS].	5	
CC6.6	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems.	5	
CC6.6	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC6.6	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	
CC6.6	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
CC6.6	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Wireless Link Protection	NET-12.1	Mechanisms exist to protect external and internal wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, inctuding scanning for unauthorized wireless access points and taking appropriate action. If an unauthorized connection is discovered.	5	
CC6.6	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
CC6.6	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
CC6.6-POF1	Restricts Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 monitor and control communications at the external network.	5	
CC6.6-POF1	Restricts Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Boundary Protection Data Flow Enforcement –	NET-03	boundary and at key internal boundaries within the network. Mechanisms exist to design, implement and review firewall and router	5	
CC6.6-POF1	Restricts Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Access Control Lists (ACLs)	NET-04	configurations to restrict connections between untrusted networks and internal systems. Mechanisms exist to configure firewall and router configurations to deny network	5	
CC6.6-POF1	Restricts Access Protects Identification and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
CC6.6-POF2	Authentication Credentials	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC6.6-POF2	Protects Identification and Authentication Credentials	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
CC6.6-POF2	Protects Identification and Authentication Credentials	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC6.6-POF2	Protects Identification and Authentication	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Password-Based Authentication	IAC-10.1	Hechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
CC6.6-POF2	Credentials Protects Identification and Authentication	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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).	5	
CC6.6-POF2	Credentials Protects Identification and Authentication	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open,	5	
CC6.6-POF2	Credentials Protects Identification and Authentication	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Electronic Messaging	NET-13	public networks. Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
CC6.6-POF3	Credentials Requires Additional	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identity & Access	IAC-01	Mechanisms exist to facilitate the implementation of identification and access	5	
CC6.6-POF3	Authentication or Requires Additional Authentication or Credentials	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management (IAM) Authenticate, Authorize and Audit (AAA)	IAC-01.2	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-POF3	Requires Additional Authentication or Credentials	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Timid-party Februlogy Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5	
CC6.6-POF3	Requires Additional Authentication or Credentials	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Adaptive Identification & Authentication	IAC-13	Mechanisms exist to allow individuals to utilize alternative methods of authentication under specific circumstances or situations.	5	
CC6.6-POF3	Requires Additional Authentication or	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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).	5	
CC6.6-POF3	Credentials Requires Additional Authentication or	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC6.6-POF3	Credentials Requires Additional Authentication or	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
CC6.6-POF3	Credentials Requires Additional Authentication or	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Remote Access	NET-14	exception). Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
CC6.6-POF4	Credentials Implements Boundary Protection Systems	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Network Security Controls	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
CC6.6-POF4	Implements Boundary Protection Systems	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(NSC) Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	5	
CC6.6-POF4	Implements Boundary	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC6.6-POF4	Protection Systems Implements Boundary	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Managed Access Control	NET-14.3	Doundary 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	
CC6.7	Protection Systems N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Points Unsupported Internet	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run	5	
CC6.7	N/A N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Browsers & Email Clients Transmission Confidentiality	CFG-04.2 CRY-03	on systems. Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Confidentiality Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
					sociality				



Secure Controls Framework (SCF) 22 of 4

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Use of External Technology Assets,	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and	5	
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Applications and/or Portable Storage Devices	DCH-13.2	transmit rists Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
					Centralized Management		Mechanisms exist to implement and govern Mobile Device Management (MDM)		
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Of Mobile Devices	MDM-01	controls. Cryptographic mechanisms exist to protect the confidentiality and integrity of	5	
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Based Encryption	MDM-03	information on mobile devices through full-device or container encryption. Mechanisms exist to protect the confidentiality, integrity and availability of electronic	5	
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Electronic Messaging	NET-13	messaging communications. Mechanisms exist to develop, document and maintain secure baseline	5	
CC6.7-POF1	Restricts the Ability to Perform Transmission	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Baseline Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
CC6.7-POF1	Restricts the Ability to Perform Transmission	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC6.7-POF1	Restricts the Ability to Perform Transmission	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Prevent Unauthorized Exfiltration	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	5	
CC6.7-POF1	Restricts the Ability to Perform Transmission Restricts the Ability to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Deny Traffic by Default & Allow Traffic by Exception End-User Messaging	NET-04.1	traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
CC6.7-POF1	Perform Transmission Restricts the Ability to	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	intersects with	Technologies Data Loss Prevention	NET-12.2 NET-17	Mechanisms exist to prohibit the transmission of unprotected sensitive/regulated data by end-user messaging technologies. Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect	5	
CC6.7-POF1	Perform Transmission Uses Encryption Technologies or Secure	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	(DLP) Use of Cryptographic	CRY-01	sensitive information as it is stored, transmitted and processed. Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
	Communication Channels Uses Encryption				Controls		Cryptographic mechanisms exist to protect the confidentiality of data being		
CC6.7-POF2	Technologies or Secure Communication Channels Uses Encryption	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Confidentiality	CRY-03	transmitted. Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
CC6.7-POF2	Technologies or Secure Communication Channels Uses Encryption	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Encrypting Data At Rest	CRY-05	Mechanisms exist to facilitate the implementation of data protection controls.	5	
CC6.7-POF2	Technologies or Secure Communication Channels	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection	DCH-01	, , , , , , , , , , , , , , , , , , , ,	5	
CC6.7-POF3	Protects Removal Media	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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. Mechanisms exist to facilitate the implementation of cryptographic protections	5	
CC6.7-POF3	Protects Removal Media	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Use of Cryptographic Controls	CRY-01	controls using known public standards and trusted cryptographic technologies.	10	
CC6.7-POF3	Protects Removal Media	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to ohvsical safeguards. Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
CC6.7-POF3 CC6.7-POF3	Protects Removal Media Protects Removal Media	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional 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	
CC6.7-POF3	Protects Removal Media	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 accentable usage parameters.	10	
CC6.7-POF3	Protects Removal Media	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Portable Storage Devices Enterprise Device	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
CC6.7-POF4		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management (EDM) Centralized Management	END-01	Mechanisms exist to facilitate the implementation of Enterprise Device Management [EDM] controls. Mechanisms exist to implement and govern Mobile Device Management (MDM)	5	
CC6.7-POF4		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Of Mobile Devices	MDM-01	controls. Mechanisms exist to prohibit unauthorized changes, unless organization-approved	5	
CC6.8	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Prohibition Of Changes Malicious Code Protection	CHG-02.1	change requests are received. Mechanisms exist to utilize antimalware technologies to detect and eradicate	5	
CC6.8	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(Anti-Malware)	END-04	msilicious code. Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to	5	
CC6.8	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Endpoint File Integrity Monitoring (FIM)	END-06	detect and report on unauthorized changes to selected files and configuration settings.	5	
CC6.8	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network	5	
CC6.8	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC6.8	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC6.8	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	
CC6.8-POF1	Restricts Installation and Modification of Application and Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	
CC6.8-POF1	Restricts Installation and Modification of Application and Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Restrict Roles Permitted To Install Software	CFG-05.2	Mechanisms exist to configure systems to prevent the installation of software, unless the action is performed by a privileged user or service.	5	
CC6.8-POF1	Restricts Installation and Modification of Application and Software Detects Unauthorized	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	
CC6.8-POF2	Changes to Software and Configuration Parameters	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Unauthorized Installation Alerts	CFG-05.1	Mechanisms exist to configure systems to generate an alert when the unauthorized installation of software is detected.	5	
CC6.8-POF2	Configuration Parameters	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Software Installation Alerts	END-03.1	Mechanisms exist to generate an alert when new software is detected.	5	
CC6.8-POF3	Uses a Defined Change Control Process Uses a Defined Change	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change Management Program Configuration Change	CHG-01	Mechanisms exist to facilitate the implementation of a change management program. Machanisms exist to govern the technical configuration change control processes.	5	
CC6.8-POF3	Control Process Uses Antivirus and Anti-	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Change Control Malicious Code Protection	CHG-02	Mechanisms exist to govern the technical configuration change control processes. Mechanisms exist to utilize antimalware technologies to detect and eradicate	5	
CC6.8-POF4	Malware Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	(Anti-Malware)	END-04	maticious code. Mechanisms exist to ensure that anti-matiware technologies are continuously	10	
CC6.8-POF5	Scans Information Assets From Outside the Entity for Malware and Other Unauthorized Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-maiware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	10	
CC7.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	5	
CC7.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	
CC7.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Integrity Checks	END-06.1	consistent with industry-accepted system hardening standards. Mechanisms exist to validate configurations through integrity checking of software and firmware.	5	
CC7.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	File Integrity Monitoring	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection	5	
					(FIM)		technology, on critical assets to generate alerts for unauthorized modifications. Mechanisms exist to detect vulnerabilities and configuration errors by routine		
CC7.1	N/A Uses Defined	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Vulnerability Scanning Configuration	VPM-06	vulnerability scanning of systems and applications. Mechanisms exist to facilitate the implementation of configuration management	5	
CC7.1-POF1	Configuration Standards Uses Defined	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management Program Secure Baseline	CFG-01	controls. Mechanisms exist to develop, document and maintain secure baseline	5	
CC7.1-POF1	Configuration Standards	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	



Secure Controls Framework (SCF) 23 of

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (ontional)	Notes (optional)
CC7.1-POF1	Uses Defined Configuration Standards	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
CC7.1-POF2	Monitors Infrastructure and Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.1-POF2	Monitors Infrastructure and Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection	5	
CC7.1-POF3	Implements Change- Detection Mechanisms	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.1-POF3	Implements Change- Detection Mechanisms	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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-POF4	Detects Unknown or Unauthorized Components	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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.	5	
CC7.1-POF4	Detects Unknown or Unauthorized Components	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
CC7.1-POF4	Detects Unknown or Unauthorized	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	File Integrity Monitoring (FIM)	MON-01.7	securings. 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	Components Conducts Vulnerability Scans	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	10	
CC7.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
CC7.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
CC7.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Inbound & Outbound Communications Traffic	MON-01.3		5	
CC7.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Wireless Intrusion Detection System (WIDS)	MON-01.5	Mechanisms exist to utilize Wireless Intrusion Detection / Protection Systems (WIDS / WIPS) to identify rogue wireless devices and to detect attack attempts via wireless networks.	5	
CC7.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Host-Based Devices	MON-01.6	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS/ 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	
CC7.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
CC7.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities	5	
CC7.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security Concept Of Operations (CONOPS)	OPS-02	Mechanisma 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	
CC7.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
CC7.2-POF1	Implements Detection Policies, Procedures, and Tools	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	
CC7.2-POF1	Implements Detection Policies, Procedures, and Tools	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.2-POF1	Implements Detection Policies, Procedures, and Tools	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.2-POF1	Implements Detection Policies, Procedures, and Tools	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.2-POF2	Designs Detection Measures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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-POF2	Designs Detection Measures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to elerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	
CC7.2-POF2	Designs Detection Measures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.2-POF2	Designs Detection Measures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
CC7.2-POF3	Implements Filters to Analyze Anomalies	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Intrusion Detection & Prevention Systems (IDS &	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	IPS) 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	
CC7.2-POF3	Implements Filters to Analyze Anomalies	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
CC7.2-POF4	Monitors Detection Tools for Effective Operation	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection policies and standards.	5	
CC7.2-POF4	Monitors Detection Tools for Effective Operation	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection Controls Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
CC7.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
CC7.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Operations	IRO-01	facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	



Secure Controls Framework (SCF) 24 of

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
CC7.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis: (4) Containment; (5) Eradication; and (6) Recovery	5	
CC7.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	5	
CC7.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets,	5	
CC7.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Incident Response & Recovery Capabilities	TPM-11	Applications. Services and/or Data (TAASD). Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	
CC7.3-POF1	Responds to Security Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
CC7.3-POF1	Responds to Security Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and	5	
CC7.3-POF1	Responds to Security Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	(6) Recovery Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
CC7.3-POF2	Communicates and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Situational Awareness For Incidents	IRO-09	Response risin (IIP) of all stakeholders. Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	
CC7.3-POF2	Communicates and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
CC7.3-POF2		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.3-POF3	Develops and Implements Procedures to Analyze Security Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation: (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and	10	
CC7.3-POF4	Assesses the Impact on Confidential Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation: (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (6) Eradication; and	5	
CC7.3-POF4	Assesses the Impact on Confidential Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	5	
CC7.3-POF5	Determines Confidential Information Used or Disclosed	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake:	5	
CC7.3-POF5	Determines Confidential Information Used or Disclosed	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	5	
CC7.3-POF6	Assesses the Impact on Personal Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated award detection or manual incident report inteke:	5	
CC7.3-POF6	Assesses the Impact on Personal Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring: (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
CC7.3-POF7	Information Used or Disclosed	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated awart detection or manual incident report intoker	5	
CC7.3-POF7	Information Used or Disclosed	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.3-POF7	Determines Personal Information Used or Disclosed	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents. Mechanisms exist to cover:	5	
CC7.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	(1) Preparation; [2] Automated event detection or manual incident report intake; [3] Analysis; [4] Containment; [5] Eradication; and	5	
CC7.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5	
CC7.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	
CC7.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
CC7.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner. Mechanisms exist to provide cybersecurity and data protection incident information	5	
CC7.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to the incident. Mechanisms exist to establish a direct, cooperative relationship between the	5	
CC7.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects 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	
CC7.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Enforcement Contacts	IRO-14	recommisms exist to maintain incluent response contacts with applicable regulatory and law enforcement agencies. Mechanisms exist to remediate risks to an acceptable level.	5	
CC7.4	N/A Assigns Roles and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Remediation Defined Roles &	RSK-06	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
CC7.4-POF1	Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Responsibilities	HRS-03	Mechanisms exist to implement and govern processes and documentation to	5	
CC7.4-POF1	Assigns Roles and Responsibilities Assigns Roles and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Operations	IRO-01	Tacilitate an organization-wide response capability for cybersecurity and data protection-related incidents. Mechanisms exist to cover:	5	
CC7.4-POF1	Assigns Rotes and Responsibilities Assigns Rotes and Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	intersects with	Incident Handling Incident Response Plan (IRP)	IRO-02 IRO-04	(1) Preparation; 17) Automated event detection or manual incident report intake: Mechanisms exist to maintain and make available a current and viable incident Response Plan (IRP) to all stakeholders.	5	
		1	1	1	6-10.3		I	I	I.



Secure Controls Framework (SCF) 25 of 4

CC7.4-POF2	ns and Responds to curity incidents in a and Responds to curity incidents as Ongoing Security Incidents as Ongoing Security Incidents as Ongoing Security Incidents as Ongoing Security Incidents are Ongoing Security Incidents as Ongoing Security Incidents as Ongoing Security Incidents as Ongoing Security Incidents as of the Security Incidents are of the Security Incidents as of the Security Incidents are of the Security Incidents as of the Security Incidents are of the Security Inci	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	intersects with	Integrated Security Incident Response Team (SSRI) Incident Response Plan (RPP) Incident Response Plan (RPP) Incident Handling Incident Handling Incident Handling Incident Response Plan (RPP) Incident Response Plan (RPP) Incident Response Plan (RPP) Incident Handling Incident Handling Incident Handling Incident Handling Incident Response Plan (RPP)	IRO-01 IRO-02 IRO-02 IRO-04 IRO-01 IRO-02 IRO-01 IRO-02 IRO-04 IRO-01	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident resources consistent in the control of the contro	(optional) 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	
CC7.4-POF2 Securi CC7.4-POF2 Contains a Securi CC7.4-POF2 Contains a Securi CC7.4-POF3 Miligates Contains a In Miligates Contains a In Miligates Contains a In	curity incidents ns and Responds to curity incidents ns and Responds to curity incidents as and Responds to curity incidents es Ongoing Security incidents tocidents solves Security incidents solves Security incidents tores Operations tores Operations tores Operations tores Operations	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional Functional Functional Functional Functional Functional Functional Functional	intersects with	Incident Response Operations Incident Handling Incident Response Plan (RP) Incident Response Plan (RP) Incident Handling Incident Handling Incident Handling Incident Handling Incident Response Plan (RP) Incident Handling Incident Response Plan (RP) Incident Response Plan (RP) Business Continuity Business Continuity	IRO-02 IRO-04 IRO-04 IRO-01 IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data grotection-related incidents. (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (6) Containment; (7) Endication; and (8) Endication; and (9) Endicati	5 5 5 5 5 5	
CC7.4-POF2 Contains Securi Securi CC7.4-POF3 Mitigates CC7.4-POF3 In CC7.4-POF4 Reaction In CC7.4-POF4 Reaction In CC7.4-POF4 Reaction In CC7.4-POF5 Restore CC7.4-POF6 Restore CC7.4-PO	ns and Responds to curity Incidents ns and Responds to curity Incidents ns and Responds to curity Incidents es Ongoing Security Incidents es Operations tores Operations tores Operations tores Operations	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional Functional Functional Functional Functional Functional Functional	intersects with	Incident Handling Incident Response Plan (RP) Incident Response Operations Incident Handling Incident Response Operations	IRO-04 IRO-02 IRO-04 IRO-01	Mechanisms exist to cover: (1) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (5) Eradication; and (5) Eradication; and (5) Eradication; and (6) Eradication; and (7) Eradication; and (8) Eradication; and (9) Eradication; and (10) Eradication; (11) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Eradication; and (7) Eradication; and (8) Eradication; and (9) Eradication; and (1) Eradication; and (2) Eradication; and (3) Eradication; and (4) Eradication; and (5) Eradication; and (6) Eradication; and (7) Eradication; and (8) Eradication; and (8) Eradication; and (9) Eradication; and (1) Eradication; and (1) Eradication; and (1) Eradication; and (1) Eradication; and (2) Eradication; and (3) Eradication; and (4) Eradication; and (5) Eradication; and (6) Eradication; and (7) Eradication; and (8) Eradication;	5 5 5	
CC7.4-POF5	curity incidents es Ongoing Security Incidents solves Security Incidents solves Security Incidents solves Security Incidents tores Operations tores Operations tores Operations	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional Functional Functional Functional Functional	intersects with intersects with intersects with intersects with intersects with intersects with	Incident Response Operations Incident Handling Incident Handling Incident Response Plan Incident Response Plan Incident Response Plan Incident Handling Incident Response Plan Incident Continuity Business Continuity Business Continuity	IRO-01 IRO-02 IRO-04 IRO-01	Nechanisms exist to maintain and make available a current and viable incident Reaponse Plan IRP to all stakeholders. Nechanisms exist to implement and govern processes and documentation to textilitate an organization-wide response capability for cybersecurity and data aratection-related incidents. (1) Preparation; (2) Automated went detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and incidents are all assessment of the processes and documentation to facilitate and organization-wide response Plan IRP) to all stakeholders. Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data crotection-related incidents. Mechanisms exist to over: (1) Preparation; (2) Automated went detection or manual incident report intake; (3) Analysis; (4) Containment;	5 5 5	
CC7.4-POF3	Incidents es Ongoing Security Incidents es Ongoing Security Incidents es Ongoing Security Incidents solves Security Incidents solves Security Incidents tories Operations	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional Functional Functional Functional Functional	intersects with intersects with intersects with intersects with intersects with	Operations Incident Handling Incident Response Plan (RP) Incident Response Operations Incident Handling Incident Handling Incident Response Plan (RP) Business Continuity Business Continuity	IRO-02 IRO-04 IRO-01	Incitation an organization-wide response capability for cybersecurity and data organization-mide incidents. Mechanisms exist to cover: (1) Preparation; (2) Automated went detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Eradication; and (7) Examination; (6) Eradication; and (7) Examination; (7) Examination; (8) Examination; (8) Examination; (8) Examination; (8) Examination; (8) Examination; (9) Examination; (1) Examination; (1) Examination; (1) Preparation; (2) Automated went detection or manual incident report intake; (3) Analysis; (4) Containment;	5 5 5	
CC7.4-POF3 Mitigation C	es Ongoing Security Incidents solves Security Incidents solves Security Incidents solves Security Incidents solves Security Incidents tores Operations tores Operations tores Operations tores Operations	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional Functional Functional Functional	intersects with intersects with intersects with intersects with	Incident Response Plan (RPP) Incident Response Operations Incident Handling Incident Response Plan (RPP) Business Continuity	IRO-04 IRO-01	(1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (6) Benneme (7) Benneme (8) Benneme (9) Be	5	
CC7.4-POF4 Resolt	Incidents solves Security incidents solves Security incidents solves Security incidents tores Operations tores Operations tores Operations tores Operations	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional Functional	intersects with	Incident Response Operations Incident Handling Incident Response Plan (IRP) Business Continuity	IRO-01	Nechanisms exist to maintain and make available a current and viable incident Reagones Plan (1870 to all stakeholders). Mechanisms exist to implement and govern processes and documentation to teclibitate an organization-wide response capability for cybersecurity and data grotection-related incidents. Wechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment;	5	
CC7.4-POF4 In	Incidents solves Security Incidents solves Security Incidents tores Operations tores Operations tores Operations	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	intersects with	Operations Incident Handling Incident Response Plan (RP) Business Continuity	IRO-02	facilitate an organization-wide response capability for cybersecurity and data protection-related incidents. Mechanisms exist to cover: (1) Preparation; (2) Automated went detection or manual incident report intake; (3) Analysis; (4) Containment;		
CC7.4+OF5 Restore CC7.4+OF5 Restore CC7.4+OF5 Restore CC7.4+OF5 Restore CC7.4+OF5 Restore CC7.4+OF6 Restore	Incidents solves Security Incidents tores Operations tores Operations tores Operations tores Operations	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	intersects with	Incident Response Plan (IRP) Business Continuity		(1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment;	5	
CC7.4-POF5 Restore CC7.4-POF5 Restore CC7.4-POF5 Restore CC7.4-POF5 Restore CC7.4-POF5 Restore CC7.4-POF6 Restore CC7.4-POF6 Restore CC7.4-POF6 Restore CC7.4-POF6 Restore CC7.4-POF6 Restore CC7.4-POF6 Restore	Incidents tores Operations tores Operations tores Operations	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional		(IRP) Business Continuity	IRO-04	(6) Recovery		
CC7.4-POF5 Restore	tores Operations tores Operations tores Operations	Download AICPA's Trust Services Criteria (TSC) for specific control wording.		intersects with			Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
CC7.4-POF5 Restore CC7.4-POF5 Restore CC7.4-POF6 Comm Securi	tores Operations tores Operations		Functional	1	Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
CC7.4-POF5 Restore CC7.4-POF6 Comm Securi Develops:	tores Operations	Download AICPA's Trust Services Criteria (TSC) for specific control wording.		intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
CC7.4-POF6 Comm Securi Develops :			Functional	intersects with	Incident Handling	IRO-02	Andersourin Hanton Indicates. (I) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery	5	
CC7.4-POF6 Comm Securi Develops	ps and Implements	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
	curity Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
	pps and Implements mmunication of curity Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated execut detection or manual incident report intake:	5	
CC7.4-POF6 Comm	pps and Implements	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.4-POF6 Comm	ops and Implements mmunication of curity Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	
CC7.4-POF6 Comm Securi	curity Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
CC7.4-POF6 Comm Securi	pps and Implements mmunication of curity Incidents as Understanding of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner. Mechanisms exist to implement and govern processes and documentation to	5	
CC7.4-POF7 Nature of Determine	re of Incident and mines Containment Strategy	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Operations	IRO-01	facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
CC7.4-POF7 Nature of Determining S	Strategy	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Constriences.	5	
CC7.4-POF7 Nature of Determine	ns Understanding of tre of Incident and mines Containment Strategy	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7 4 POEs Remedia		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
CC7.4-POF8 Vuln	/ulnerabilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation: (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Renneuro	5	
CC7.4-POF8 Vuln	/ulnerabilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 remediate risks to an acceptable level.	5	
CC7.4-POF8 Vuln	/ulnerabilities ediates Identified	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Remediation Vulnerability Remediation	RSK-06 VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and	5	
Vuln	Communicates	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Process Incident Response Operations		remediated. Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
CC7.4-POF9 Remedia	ediation Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation: (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (6) Eradication; and (6) Benomen.	5	
	Communicates ediation Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
	Communicates ediation Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	
	Communicates ediation Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
CC7.4-POF10 Effectiver		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Contingency Plan Root Cause Analysis (RCA) &	BCD-05	Nechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
Eval	Response Evaluates the iveness of Incident	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data	5	
Eval	Response Evaluates the	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Operations Incident Handling	IRO-02	protection-related incidents. Mechanisms exist to cover: (1) Preparation: (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (6) Endiclation;	5	



Secure Controls Framework (SCF) 26 of 4

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
CC7.4-POF10		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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.	(optional) 5	
CC7.4-POF10	Response Evaluates the Effectiveness of Incident	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of	5	
CC7.4-POF11	Response Periodically Evaluates	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response	IRO-01	future incidents. Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data	5	
CC7.4-POF11	Incidents Periodically Evaluates	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Operations Incident Handling	IRO-02	protection-related incidents. Mechanisms exist to cover: (1) Preparation:	5	
CC7.4-POF11	Incidents Periodically Evaluates	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Plan	IRO-04	(7) Automated event detection or manual incident report inteker Mechanisms exist to maintain and make available a current and viable incident Response Plan (IRP) to all stakeholders.	5	
CC7.4-POF11	Incidents Periodically Evaluates	Downtoad AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(IRP)	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments,	5	
CC7.4-POF12	Incidents Applies Breach Response	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response	IRO-01	as necessary. Mechanisms exist to implement and govern processes and documentation to	5	
CC7.4-POF12	Procedures	Download AICPA'S Trust Services Citteria (1SC) for specific control wording.	Functional	intersects with	Operations	INO-01	facilitate an organization-wide response capability for cybersecurity and data orotection-related incidents. Mechanisms exist to cover:	•	
CC7.4-POF12	Applies Breach Response Procedures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	(1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and	5	
CC7.4-POF12	Applies Breach Response Procedures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.4-POF13	Disclosure	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
CC7.4-POF13	Disclosure	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated exert detection or manual incident report intake:	5	
CC7.4-POF13	Communicates	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.4-POF13	Communicates Unauthorized Use and Disclosure Communicates	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisma exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities. Mechanisma exist to report sensitive/regulated data incidents in a timely manner.	5	
CC7.4-POF13	Unauthorized Use and Disclosure	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2		5	
CC7.4-POF14	Application of Sanctions	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Personnel Sanctions Business Continuity	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures. Mechanisms exist to facilitate the implementation of contingency planning controls	10	
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management System (BCMS)	BCD-01	to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Resume All Missions & Business Functions Continue Essential	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation. Mechanisms exist to continue essential missions and business functions with little	5	
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Mission & Business Functions Resume Essential	BCD-02.2	or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites.	5	
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	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	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	intersects with	Ongoing Contingency Planning	BCD-06	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services) (3) Technologies (e.g., new, altered or decommissioned technologies); (4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or (6) Feedback from contingency plan testing activities.	5	
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 Technology	5	
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Backup & Restoration Hardware Protection Business Continuity	BCD-13	Mechanisms exist to protect backup and restoration hardware and software. Mechanisms exist to facilitate the implementation of contingency planning controls	5	
CC7.5-POF1	Restores the Affected Environment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Management System (BCMS)	BCD-01	to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) otavbooks).	10	
CC7.5-POF1	Restores the Affected Environment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	5	
CC7.5-POF1	Restores the Affected Environment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.5-POF1	Restores the Affected Environment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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-POF1	Restores the Affected Environment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
CC7.5-POF2	Communicates Information About the Incident	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/OR) playbooks).	10	
CC7.5-POF2	Communicates Information About the Incident	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC7.5-POF2	Incident	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
CC7.5-POF3	Determines Root Cause of the Incident	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	10	
CC7.5-POF4	Implements Changes to Prevent and Detect Recurrences	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
CC7.5-POF4	Implements Changes to Prevent and Detect Recurrences	Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	intersects with	Ongoing Contingency Planning	BCD-06	Mechanisms exist to update contingency plans due to changes affecting: [1) People (e.g., personnel changes); [2) Processes (e.g., new, altered or decommissioned business practices, including third-party services); [3) Technologies (e.g., new, altered or decommissioned technologies); [4] Date (e.g., changes to data flows and/or data repositories); [5] Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or glamping to the procession of the proces	5	
CC7.5-POF5	Improves Response and Recovery Procedures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	



Secure Controls Framework (SCF) 27 of

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CC7.5-POF5	Improves Response and Recovery Procedures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Ongoing Contingency Planning	BCD-06	Mechanisma exist to undate contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, attered or decommissioned business practices, including third-party services) (3) Technologies (e.g., new, attered or decommissioned technologies);	5	
					-		(4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or (6) Feedback from contingency plan testing activities.		
CC7.5-POF6	Implements Incident- Recovery Plan Testing	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	10	
CC8.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
CC8.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	
CC8.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
CC8.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
CC8.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
CCB.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Stakeholder Notification of Changes Secure Development Life	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5	
CCB.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
CC8.1-POF1	Manages Changes Throughout the System Life Cycle	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
CC8.1-POF1	Manages Changes Throughout the System Life Cycle	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
CC8.1-POF2	Authorizes Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 Authorizes Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	intersects with	Configuration Change Control	CHG-02 CHG-02.1	Mechanisms exist to govern the technical configuration change control processes. Mechanisms exist to prohibit unauthorized changes, unless organization-approved	5	
CC8.1-POF2	Authorizes Changes Authorizes Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Prohibition Of Changes Access Restriction For	CHG-02.1	change requests are received. Mechanisms exist to enforce configuration restrictions in an effort to restrict the	5	
CC8.1-POF3	Designs and Develops	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change Change Management	CHG-01	ability of users to conduct unauthorized changes. Mechanisms exist to facilitate the implementation of a change management	5	
CC8.1-POF3	Changes Designs and Develops Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Program Configuration Change Control	CHG-02	program. Mechanisms exist to govern the technical configuration change control processes.	5	
CC8.1-POF3	Designs and Develops Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Representative for Asset Lifecycle	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data privacy representative in the configuration change control review process.	5	
CC8.1-POF3	Designs and Develops Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Changes Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5	
CC8.1-POF4	Documents Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
CC8.1-POF4	Documents Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
CC8.1-POF4	Documents Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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-POF5	Tracks System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change Management Program Configuration Change	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
CC8.1-POF5	Tracks System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	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	
CC8.1-POF5	Tracks System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Test, Validate & Document Changes	CHG-02.2	production environment before changes are implemented in a production environment.	5	
CC8.1-POF6	Configures Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC8.1-POF6	Configures Software Configures Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Control Configuration	CHG-02 CFG-01	Mechanisms exist to facilitate the implementation of configuration management	5	
CC8.1-POF6	Configures Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management Program Secure Baseline	CFG-02	controls. Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	
CC8.1-POF6	Configures Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configurations Automated Central Management &	CFG-02.2	consistent with industry-accepted system hardening standards. Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous	5	
CC8.1-POF7		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Verification Change Management	CHG-01	Diagnostics and Mitigation (CDM), or similar technologies. Mechanisms exist to facilitate the implementation of a change management program.	5	
CC8.1-POF/	rests System Changes	DOWNLOSS ALCEPA'S TRUST Services Criteria (TSC) for specific control wording.	Functional	intersects with	Program	CHG-UI	Mechanisms exist to govern the technical configuration change control processes.		
CC8.1-POF7	Tests System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to appropriately test and document proposed changes in a non-	5	
CC8.1-POF7	Tests System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Test, Validate & Document Changes	CHG-02.2	production environment before changes are implemented in a production environment.	5	
CC8.1-POF8		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	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.	10	
CC8.1-POF8	Approves System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes. Mechanisms exist to facilitate the implementation of a change management	10	
CC8.1-POF9	Deploys System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change Management Program Configuration Change	CHG-01	program. Mechanisms exist to govern the technical configuration change control processes.	5	
CC8.1-POF9		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Change Control Access Restriction For	CHG-02	Mechanisms exist to enforce configuration restrictions in an effort to restrict the	5	
CC8.1-POF9	. , , ,	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change	CHG-04	ability of users to conduct unauthorized changes. Mechanisms exist to limit operational privileges for implementing changes.	5	
CC8.1-POF9	Deploys System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes. Mechanisms exist to facilitate the implementation of a change management	5	
CC8.1-POF10	Identifies and Evaluates System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change Management Program	CHG-01	program.	5	
CC8.1-POF10	Identifies and Evaluates System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
CC8.1-POF10	Identifies and Evaluates System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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-POF10	Identifies and Evaluates System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5	
CC8.1-POF10	Identifies and Evaluates System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Automated Access Enforcement / Auditing	CHG-04.1	Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes.	5	
CC8.1-POF11	Identifies Changes in Infrastructure, Data, Software, and Procedures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
CC8.1-POF11	Identifies Changes in Infrastructure, Data, Software, and Procedures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
CC8.1-POF11	Identifies Changes in Infrastructure, Data,	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Automated Access Enforcement / Auditing	CHG-04.1	Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes.	5	
	Software, and Procedures	1	1	1			ı	1	ı



Secure Controls Framework (SCF) 28 of

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
	Identifies Changes in Infrastructure, Data,				Automated Central		Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous	(opaonat)	
CC8.1-POF11	Required to Remediate Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management & Verification	CFG-02.2	Diagnostics and Mitigation (CDM), or similar technologies.	5	
CC8.1-POF12	Creates Baseline Configuration of IT Creates Baseline	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls. Mechanisms exist to develop, document and maintain secure baseline	5	
CC8.1-POF12	Configuration of IT Technology	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Baseline Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
CC8.1-POF13	Provides for Changes Necessary in Emergency Situations	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
CCB.1-POF13	Provides for Changes Necessary in Emergency	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
CC8.1-POF13	Situations Provides for Changes Necessary in Emergency	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Test, Validate & Document	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	
CC8.1-POF13	Situations Provides for Changes Necessary in Emergency	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Changes	IAC-15.9	environment. Mechanisms exist to establish and control "emergency access only" accounts.	5	
CC8.1-POF13	Situations Manages Patch Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Emergency Accounts Change Management	CHG-01	Mechanisms exist to facilitate the implementation of a change management	5	
CCB.1-POF14	Manages Patch Changes		Functional	intersects with	Program Configuration Change Control	CHG-02	program. Mechanisms exist to govern the technical configuration change control processes.	5	
CC8.1-POF14	Manages Patch Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Vulnerability & Patch Management Program	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
CC8.1-POF14	Manages Patch Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(VPMP) Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
CC8.1-POF15	Considers System	Described MODAL Tour Control of College (COC) to a series of the control of Coc	Functional	intersects with	Business Continuity	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g.,	5	
CC8.1-POF15	Resilience	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management System (BCMS)	BCD-01	Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	,	
CC8.1-POF15	Considers System Resilience	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
CC8.1-POF15	Considers System Resilience	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
CC8.1-POF16	Protects Confidential Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
CC8.1-POF16	Protects Confidential	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Test, Validate & Document	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	
	Information Protects Confidential				Changes		production environment before changes are implemented in a production environment. Mechanisms exist to facilitate the implementation of data protection controls.		
CC8.1-POF16	Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection Vulnerability & Patch	DCH-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability	5	
CC8.1-POF16	Protects Confidential Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management Program (VPMP)	VPM-01	management controls.	5	
CC8.1-POF16	Protects Confidential Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
CC8.1-POF17	Protects Personal Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
CC8.1-POF17	Protects Personal Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
CC8.1-POF17	Protects Personal Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are	5	
CC8.1-POF18	Privacy by Design	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Data Privacy Program	PRI-01	processed lawfully fairly and transparently. Mechanisms exist to facilitate the implementation and operation of data protection.	10	
CC8.14FOF18	Filvacy by Design	DOWNLOAD AICHAS HIBS SERVICES CITIENS (1907) to specific control wording.	Pulictional	Subset 01		FRIOT	controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are orocessed lawfullv. fairly and transparently. Mechanisms exist to minimize the collection of Personal Data (PD) to only what is	10	
CC8.1-POF18	Privacy by Design	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	5	
CC8.1-POF18	Privacy by Design	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, update and/or share Personal Data (PD), either generally or in support of a specific business process.	5	
CC8.1-POF18	Privacy by Design	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cyber security and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Continuity Management System	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g.,	5	
					(BCMS)		Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) Dlavbooks). Mechanisms exist to implement alternative or compensating controls to satisfy		
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Alternative Security Measures	BCD-07	security functions when the primary means of implementing the security function is unavailable or compromised.	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	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.	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to develop and keep current a catalog of applicable risks	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Catalog	RSK-03.1	associated with the organization's business operations and technologies in use. Mechanisms exist to implement a threat intelligence program that includes a cross-	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Threat Intelligence Feeds 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,	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Threat Catalog	THR-09	threat 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	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	external threats to the organization, both natural and mammade. Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Value services. Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Acquisition Strategies,	TPM-03.1	those risks and threats, as necessary. Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets. Applications	5	
CC9.1	N/A	Download AICPA's trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Tools & Methods Limit Potential Harm	TPM-03.1	and/or Services (TAAS). Mechanisms exist to utilize security safeguards to limit harm from potential	5	
CC9.1	N/A	Download AICPA's trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Processes To Address Weaknesses or	TPM-03.2	adversaries who identify and target the organization's supply chain. Mechanisms exist to address identified weaknesses or deficiencies in the security of	5	
					Deficiencies Third-Party Processing,		Mechanisms exist to restrict the location of information processing/storage based		
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Storage and Service Locations	TPM-04.4	on business requirements. Mechanisms exist to require contractual requirements for cybersecurity and data	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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. Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Monitoring for Third-Party Information Disclosure	TPM-07	of organizational information.	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data extension acetation acetation.	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Deficiency Remediation	TPM-09	and data protection controls. Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
CC9.1	N/A		Functional	intersects with	Managing Changes To	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account	5	
GC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	runctional	intersects with	Third-Party Services	1PM-10	the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.		



Secure Controls Framework (SCF) 29 of 4

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
CC9.1-POF1	Considers Mitigation of Risks of Business Disruption	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	(optional)	
CC9.1-POF1	Considers Mitigation of Risks of Business Disruption	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
CC9.1-POF1	Considers Mitigation of Risks of Business Disruption	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC9.1-POF2	Considers the Use of Insurance to Mitigate Financial Impact Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) alwhooks).	5	
CC9.1-POF2	Considers the Use of Insurance to Mitigate Financial Impact Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
CC9.1-POF2	Considers the Use of Insurance to Mitigate Financial Impact Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 Technology Assets, Applications and and/or Services (RAS), 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.	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5	
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
CC9.2-POF1	Establishes Requirements for Vendor and Business Partner Engagements	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
CC9.2-POF1	Establishes Requirements for Vendor and Business Partner Engagements	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5	
CC9.2-POF1	Establishes Requirements for Vendor and Business Partner Engagements	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
CC9.2-POF1	Establishes Requirements for Vendor and Business Partner Engagements	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Sandres (TARS) supply chains; and	5	
CC9.2-POF1	Establishes Requirements for Vendor and Business Partner Engagements	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Another hands and our department of the contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
CC9.2-POF1	Establishes Requirements for Vendor and Business Partner Engagements	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
CC9.2-POF2	Identifies Vulnerabilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
CC9.2-POF2	Identifies Vulnerabilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5	
CC9.2-POF2	Identifies Vulnerabilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC9.2-POF2	Identifies Vulnerabilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Annillations and/or Sandres (TASS) supply chains; and	5	
CC9.2-POF2	Identifies Vulnerabilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
CC9.2-POF3	Assesses Vendor and Business Partner Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
CC9.2-POF3	Assesses Vendor and Business Partner Risks	Download AIGPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5	
CC9.2-POF3	Assesses Vendor and Business Partner Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC9.2-POF3	Assesses Vendor and Business Partner Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (I) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (J) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
CC9.2-POF3	Assesses Vendor and Business Partner Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
CC9.2-POF4	Assigns Responsibility and Accountability for Managing Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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, naintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
CC9.2-POF4	Assigns Responsibility and Accountability for Managing Vendors and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC9.2-POF4	Assigns Responsibility and Accountability for Managing Vendors and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Sandoss ETAAS) supply chains: and	5	
CC9.2-POF4	Assigns Responsibility and Accountability for Managing Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Anolications and/or Sencines TEASS winds rehalves and Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	
CC9.2-POF5	Establishes Communication Protocols	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	Internal stakeholders and external service Provider's IESP'91. Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC9.2-POF5	for Vendors and Business Establishes Communication Protocols for Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
CC9.2-POF6	Partners Establishes Exception Handling Procedures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC9.2-POF6	Establishes Exception Handling Procedures From Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
CC9.2-POF6	Establishes Exception Handling Procedures From Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CC9.2-POF7	Assesses Vendor and Business Partner Performance	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 Technology Assets, Applications and/or Services (TAAS), including documenting excluded with the production of the p	5	
CC9.2-POF7	Assesses Vendor and Business Partner	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	selected mitigating actions and monitoring performance against those plans. Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5	
CC9.2-POF7	Performance Assesses Vendor and Business Partner	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC9.2-P0F7	Performance Assesses Vendor and Business Partner	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets,	5	
	Performance Assesses Vendor and				Management (SCRM)		Applications and/or Services (TAAS) supply chains: and Mechanisms exist to perform recurring validation of the Responsible, Accountable,		
CC9.2-POF7	Business Partner Performance Assesses Vendor and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Scope Review	TPM-05.5	Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity and data protection control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders. Mechanisms exist to monitor, regularly review and assess External Service Providers	5	
CC9.2-POF7	Business Partner Performance	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Review of Third-Party Services	TPM-08	(ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	5	
CC9.2-POF8	Implements Procedures for Addressing Issues Identified During Vendor and Business Partner	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 Technology Assets, Applications and/or Services (TASS, including documenting selected mitigating actions and monitoring performance against those plans.	5	
CC9.2-POF8	Assessments Implements Procedures for Addressing Issues	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC9.2-POF8	Identified During Vendor Implements Procedures for Addressing Issues	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets,	5	
	Identified During Vendor Implements Procedures for Addressing Issues						Anotherstone and/or Candeac (TASC) symptochaines and Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services		
CC9.2-POF8	Identified During Vendor and Business Partner Assessments Implements Procedures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	(TAAS). Mechanisms exist to include "break clauses" within contracts for failure to meet	5	
CC9.2-POF8	for Addressing Issues Identified During Vendor	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Break Clauses	TPM-05.7	contract criteria for cybersecurity and/or data privacy controls.	5	
CC9.2-POF8	Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	5	
CC9.2-POF8	Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC9.2-POF8	Implements Procedures for Addressing Issues Identified During Vendor and Business Partner	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5	
CC9.2-POF9	Assessments Implements Procedures for Terminating Vendor and Business Partner Relationships	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
CC9.2-POF9	Implements Procedures for Terminating Vendor	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CCS.2-FOFS	and Business Partner Relationships Implements Procedures	DOWNLOAD AICHAS THUS SERVICES CITERIA (190) TOT SPECIAL CONTOUR WORKING.	runctionat	intersects with	miliu-raity rianagement	IFINOI	Mechanisms exist to:		
CC9.2-POF9	for Terminating Vendor and Business Partner Relationships	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and "Under properties properties properties to exist the extensivation" or property to	5	
CC9.2-POF9	Implements Procedures for Terminating Vendor and Business Partner Relationships	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
CC9.2-POF9	Implements Procedures for Terminating Vendor and Business Partner Relationships	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
CC9.2-POF9	Implements Procedures for Terminating Vendor and Business Partner Relationships	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC9.2-POF9	Implements Procedures for Terminating Vendor and Business Partner Relationships	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (IPD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to subcontractors.	5	
CC9.2-POF10	Obtains Confidentiality Commitments From Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
CC9.2-POF10	Obtains Confidentiality Commitments From Vendors and Business	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC9.2-POF10	Obtains Confidentiality Commitments From	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets,	5	
CC9.2-POF10	Vendors and Business Obtains Confidentiality Commitments From Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Apolications and/or Sanciese TTASS is unother chains: and Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
CC9.2-POF10	Obtains Confidentiality Commitments From Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
CC9.2-POF10	Obtains Confidentiality Commitments From Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisma exist to obtain a First-Party Declaration (IPD) from applicable Enternal Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to subcontractors.	5	
CC9.2-POF11	Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 Technology Associates, Applications and/or Services (TASA), including documenting selected mitigating actions and monitoring performance against those plans.	5	
CC9.2-POF11	Assesses Compliance With Confidentiality Commitments of Vendors	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5	
CC9.2-POF11	Assesses Compliance With Confidentiality Commitments of Vendors	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC9.2-POF11	Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
CC9.2-P0F11	Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESP4) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to subcontractors.	5	
CC9.2-POF12	Obtains Privacy Commitments From Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 Technology, Assex, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
CC9.2-POF12	Obtains Privacy Commitments From	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC9.2-POF12	Vendors and Business Obtains Privacy Commitments From	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets,	5	
	Vendors and Business	·			management (SCRM)		Annihotine and/or Sandras (TAAS) county chains and		L



Set Theory Relationship Mapping (STRM)

Secure Controls Framework (SCF) 31 of 40

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CC9.2-POF12	Obtains Privacy Commitments From Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 and data protection controls between internal stakeholders and External Service Providers (ESPs).	(optional) 5	
CC9.2-POF12	Obtains Privacy Commitments From Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
CC9.2-POF12	Obtains Privacy Commitments From Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESP9) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to subcontractors.	5	
CC9.2-POF12	Obtains Privacy Commitments From Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	5	
CC9.2-POF13	Assesses Compliance With Privacy Commitments of Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Threat Intelligence Feeds 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, resoonse and recovery activities.	5	
CC9.2-POF13	Assesses Compliance With Privacy Commitments of Vendors	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
CC9.2-POF13	Assesses Compliance With Privacy Commitments of Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
CC9.2-POF13	Assesses Compliance With Privacy Commitments of Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compet External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely infected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	5	
CC9.2-POF13	Assesses Compliance With Privacy Commitments of Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Monitoring for Third-Party Information Disclosure	TPM-07	Mechanisms exist to monitor for evidence of unauthorized exfitration or disclosure of organizational information.	5	
CC9.2-POF13	Assesses Compliance With Privacy Commitments of Vendors and Business Partners	Download AIGPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	5	
CC9.2-POF13	Assesses Compliance With Privacy Commitments of Vendors and Business Partners	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
CC9.2-POF13	Assesses Compliance With Privacy Commitments of Vendors	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
CC9.2-POF13	Assesses Compliance With Privacy Commitments of Vendors	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
P1.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Privacy Act Statements	PRI-01.2	Mechanisms exist to provide additional formal notice to individuals from whom the information is bing collected that Includes: (1) Notice of the authority of organizations to collect Personal Data (PD); (2) Whether providing PD is mandationy or optional; (3) The principal purpose or purposes for which the PD is to be used; (4) The interded facioaures or roution uses of the information; and (5) The consequences of not providing all or some portion of the information	5	
P1.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to: (I) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPC) or similar rote; (I) Ensure that organizational data privacy practices are publicly available through organizational vebaties or document repositories; (I) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(s) regarding data privacy practices; and (I) inform data subjects when changes are made to the privacy notice and the nature	5	
P1.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Privacy Notice	PRI-02	Manch-Assonant Mechanisms esists to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and absequently as necessary. (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related or theria required by applicable statutory, regulatory and contractured or theria required by applicable statutory, regulatory and contractured or their arequired by applicable statutory, and before the society of the statutory, and the society of the	5	
P1.1-P0F1	Communicates to Data Subjects [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Privacy Notice	PRI-02	Nechanisms exist to: (I) Make data privey notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privery notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, sherve, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual colligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary;	5	
P1.1-P0F1	Communicates to Data Subjects [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Purpose Specification	PRI-02.1	To renderative view and to plane the colorate of the plane of the purpose of the	5	
P1.1-P0F2	Provides Notice to Data Subjects [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary. (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual colligations. (4) Define the scope of PD processing activities, including the geographic locations and hirt-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and	5	



Secure Controls Framework (SCF) 32 of 4

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
P1.1-P0F2	Provides Notice to Data Subjects [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Purpose Specification	PRI-02.1	Mechanisms exist to ensure the data privacy notice identifies the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted, shared.	5	
P1.1-POF3	Covers Entitles and Activities in Notice [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and absequently as necessary. (2) Ensure that data privacy notices are clear and easy-to-understand, expressing retevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and thirp-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention	5	
P1.1-P0F3	Covers Entities and Activities in Notice [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Purpose Specification	PRI-02.1	requirements. Mechanisms exist to ensure the data privacy notice identifies the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted, shared.	5	
P1.1-POF4	Uses Clear Language and Presents a Current Privacy Notice in a Location Easily Found by Data Subjects [C]	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privay notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PDI) is collected, received, processed, stored, transmitted, shinery, dupleted and disposed; (3) Contain all necessary notice-related criterial required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
P1.1-P0F4	Uses Clear Language and Presents a Current Privacy Notice in a Location Fasily	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Purpose Specification	PRI-02.1	Mechanisms exist to ensure the data privacy notice identifies the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted, shared	5	
P1.1-POF5	Reviews the Privacy Notice [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	snarer Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	
P1.1-POFS	Reviews the Privacy Notice [C]	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (I) Make data privoy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and daposed: (I) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (d) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (s) Periodically, review and update the content of the privacy notice, as necessary; and (g) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
P1.1-POF6	Communicates Changes to Notice [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to: (I) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar rote: (I) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; (I) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; (I) Ultilize publicly training email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(e) regarding data privacy practices; and (4) Inform data subjects when changes are made to the privacy notice and the nature data subjects when changes are made to the privacy notice and the nature data subjects when changes are made to the privacy notice and the nature data subjects.	5	
P1.1-P0F7	Retains Prior Notices [C]	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privey notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privery notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PDI) is collected, received, processed, stored, transmitted, shinery, dupleted and algoposet; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (6) Persolically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
P2:0	Privacy Criteria Related to Choice and Consent	Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	subset of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for upsers to decline the authorization, and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
P2.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
P2.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to process, store and/or share Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or	5	
P2.1-P0F1	Communicates to Data Subjects [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for upsers to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
P2.1-P0F2	Communicates Consequences of Denying or Withdrawing Consent [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for upsers to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
P2.1-POF3	Obtains Implicit or Explicit Consent [C]	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with the privacy risks of the authorization; (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the subcrization; and (3) All necessary choice and consent-related oriteria required by applicable statutory, regulatory and contractual obligations.	5	



Secure Controls Framework (SCF) 33 of 4

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
P2.1-P0F4	Documents and Obtains Consent for New Purposes and Uses [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to process, store and/or share Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or	5	
P2.1-POF5	Obtains Explicit Consent for Sensitive Information [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	intersects with	Choice & Consent	PRI-03	If A serificant amount of time has assess since an individual exerconsent. Mechanisms exist onesible data subjects to submorte the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (I) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for unest to decline the authorization, and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
P2.1-POF6	Obtains Consent for Data Transfers [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
P3.0	Privacy Criteria Related to Collection	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	10	
P3.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	5	
P3.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, update and/or share Personal Data (PD), either generally or in support of a specific business process.	5	
P3.1-POF1	Limits the Collection of Personal Information [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	5	
P3.1-POF2	Collects Information by Fair and Lawful Means [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal quardian consent. Mechanisms exist to minimize the collection of Personal Data (PD) to only what is	5	
P3.1-POF3	Collects Information From Reliable Sources [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	5	
P3.1-POF3	Collects Information From Reliable Sources [P][C] Informs Data Subjects When Additional	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Primary Sources Restrict Collection To	PRI-04.2	Mechanisms exist to ensure information is directly collected from the data subject, whenever possible. Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice,	5	
P3.1-POF4	Information Is Acquired [P][C] Informs Data Subjects	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identified Purpose	PRI-04	including protections against collecting PD from minors without appropriate parental or legal guardian consent. Mechanisms exist to notify affected data subjects if their Personal Data (PD) has	5	
P3.1-POF4	When Additional Information is Acquired [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Notice of Correction or Processing Change	PRI-06.2	been corrected or amended. Mechanisms exist to enable data subjects to authorize the collection, processing,	5	
P3.2	N/A	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Choice & Consent	PRI-03	storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
P3.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to process, store and/or share Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed: Or 2/1 A significant amount of time has nessent since an individual case consent	5	
P3.2-POF1	Informs Data Subjects of Consequences of Failure to Provide Consent [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Tailored Consent	PRI-03.1	Mechanisms exist to allow data subjects to modify permission to collect, receive, process, store, transmit, update and/or share selected attributes of their Personal Data (PD).	5	
P3.2-POF2	Documents Explicit Consent to Retain Information [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposed of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for upsers to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
P4.0	Privacy Criteria Related to Use, Retention, and Disposal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (I) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, detroys, erases, and/or anonymizes the Po, regardies of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originats, copies and archived records).	10	
P4.0	Privacy Criteria Related to Use, Retention, and Disposal	Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	subset of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purposely originalty collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	10	
P4.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	sechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorites the use of PD when such information is required for internal testing, training and research.	5	
P4.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
P4.1-POF1	Uses Personal Information for Intended Purposes [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating, and/or sharing Personal Data (PD) to: (1) The purposely originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
P4.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to furfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	



secure Controls Framework (SCF) 34 of 40

Mathematical Math	FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
	P4.2-P0F1		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PRI-05	[1] Retain Personal Data IPD], including metadata, for an organization-defined time period to furfill the purpose(s) identified in the notice or as required by law; [2] Dispose of, destroys, erases, and/or anonymizes the PD, regardess of the method of storage; and [3] be organization-defined techniques or methods to ensure secure deletion or	5	
March Marc	P4.2-POF2		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PRI-01.6	security safeguards that are sufficient and appropriately scoped to protect the	5	
No. No. No. No. No. No.						Data (PD)				
Part						Personal Data (PD)		Mechanisms exist to: (I) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purposety identified in the notice or as required by law; (2) lispose of, detroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deterior or		
Part	P4.3-POF1	Flags Requests for	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PRI-06.4	complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or	5	
March Marc	P4.3-POF1	Flags Requests for Deletion [PI[C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
March Marc	P4.3-POF2	and Redacts Personal Information [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Destruction or Re-Use of	AST-09	using organization-defined techniques and methods to prevent information being recovered from these components.	5	
Property	P4.3-POF2	Information [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical Media Disposal	DCH-08	formal procedures.	5	
Part	P4.3-POF2	Disposes of, Destroys,	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Information Disposal	DCH-21		5	
A 1 Prince Prin	P4.3-POF2	and Redacts Personal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PRI-05	[1] Retain Personal Data IPD], including metadata, for an organization-defined time period to furfill the purpose(s) identified in the notice or as required by law; [2] Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and [3] Use organization-defined techniques or methods to ensure secure deletion or	5	
1.100 1.00	P4.3-POF3		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Destruction or Re-Use of	AST-09	using organization-defined techniques and methods to prevent information being	5	
March Marc	P4.3-POF3	Information [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
Part 1997 Service (PDR) Service (PDR) Service (PDR) to question to the service (PDR) to question control under	P4.3-POF3		Download AlCPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Information Disposal	DCH-21		5	
P3 1 No. 97 CHISCHERISTON Overload ASCPA's hard frozend Critical (ESC) to seart common working. P3 1 No. 98 CHISCHERISTON Overload ASCPA's hard frozend Critical (ESC) to seart common working. P3 1 No. 98 CHISCHERISTON Overload ASCPA's hard frozend Critical (ESC) to seart common working. P3 1 No. 98 CHISCHERISTON Overload ASCPA's hard frozend Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard frozend Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard frozend Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard frozend Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard forever Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard forever Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard forever Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard forever Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard forever Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard forever Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard forever Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard forever Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard forever Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard forever Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard forever Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard forever Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard forever Critical (ESC) to seart common working. P3 1 No. 98 Chischeriston Overload ASCPA's hard forever Critical (ESC) to seart common working. P3 1 No.	P4.3-POF3		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PRI-05	[1] Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; [2] Dispose of, destroys, erases, and/or anonymizes the PD, regardess of the method of storage; and [3] Use organization-defined techniques or methods to ensure secure deletion or	5	
PS.1 POY1 PS.1 POY1 PS.1 POY2 And excitate Clarate (EX) for specific control wording. PS.1 POY1 PS.1 POY1 PS.1 POY2 And excitate Clarate (EX) for specific control wording. PS.1 POY2 And excitate Ps.2 Poy1 Ps.1 Poy1 Ps.1 Ps.2 Ps.2 Ps.2 Ps.2 Ps.2 Ps.2 Ps.3 Ps.2 Ps.3 Ps.3 Ps.3 Ps.3 Ps.3 Ps.3 Ps.3 Ps.3	P5.0		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of		PRI-06	(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the butten, risk or expanse of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specific or how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting,	10	
PS.1 NA. Downtoad AICPA's Trust Sources Crisine (PIC) for specific control wording. PS.1 POT2 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT2 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT2 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT3 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT3 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT3 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT3 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT3 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT3 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT3 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT3 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT3 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT4 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT4 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT4 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT4 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT4 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT4 Authorities Date Control and AICPA's Trust Sources Critical (PIC) for specific control wording. PS.1 POT4 Author	P5.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		DCH-22.1	inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-	5	
PS. 1 N/A Coversional ACPA's Trust Services Criteria (TIC) for specific control wooding. PS. 1-POT1 Responds to Dish Coversional Responds (PT) Responds to Dish Coversional Responds (PT) Responds to Dish Coversional Responds (PT) Responds to Dish Coversional Responds (PT) Responds to Dish Coversional Responds (PT) Responds to Dish Coversional Responds (PT) Responds to Dish Coversional Responds (PT) Responds to Dish Coversional Responds (PT) Responds to Dish Coversional Responds (PT) Resp	P5.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PRI-06	(1) Access their Personal Data (PD) that is being processed, stored and shared,	5	
PS.1-PGF2 Authenticates Disa Subjects (Saving) PTIC PS.1-PGF2 Authenticates Disa Subjects (Saving) PTIC PS.1-PGF3 Actions (Saving) PTIC PS.1-PGF4 Actions (Saving) PTIC PS.1-PGF4 PS.1-PGF4 Actions (Saving) PTIC PS.1-PGF4 Actions (Saving) PTIC PS.1-PGF4 PS.1-PGF4 Actions (Saving) PTIC PS.1-PGF4 Actions (Saving) PTI	P5.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PRI-06.4	complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or	5	
P5.1-POF2 Authenticates Data Subjects* Identity [P][C] Download AICPA's Trust Services Criteria (TSC) for specific control wording. P5.1-POF3 P5.1-POF3 Permits Data Subjects PF.1-POF4 Permits Data Subjects PF.1-POF4 Provides Understandable P5.1-POF4 Provides Understandable PF.1-POF4 Provides Understandable PF.1-POF4 Provides Understandable PF.1-POF4 Provides Understandable PF.1-POF4 Provides Understandable Provides Understandable Provides Understandable PF.1-POF4 PF.1-POF64 PF.1-POF64 PF.1-POF64 PF.1-POF64 PF.1-POF65 PF.1-POF64 PF.1-POF65 PF.1-POF65 PF.1-POF64 PF.1-POF65 PF.1-POF65 PF.1-POF65 PF.1-POF65 PF.1-POF66 PF.1-POF666 PF.1-POF66 PF.1-POF66 PF.1-POF666 PF	PS.1-POF1		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PP) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (3) Obtain the adoptive of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request correction to their PD and (7) Restrict the further collecting, receiving, processing, storing, transmitting,	5	
PS.1-POF3 PS.1-POF3 PS.1-POF4 PS.1-POF4 PS.1-POF4 PS.1-POF4 PS.1-POF4 PS.1-POF4 PS.1-POF64 PS.1-POF66 PS.1-POF64 PS.1-POF66 PS.1-POF	P5.1-POF2		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PRI-06	(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the buttern, risk or expanse of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request correction to their PD due to inaccuracies; (6) Request correction to their PD and (7) Restrict the further collecting, receiving, processing, storing, transmitting,	5	
PS.1-PDF4 Personal Information Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with User Feedback. Management Completed Air Services Criteria (TSC) for specific control wording. Functional intersects with User Feedback. Management Completed Air Services Criteria (TSC) for specific control wording. Functional intersects with User Feedback. Management Completed Air Services Criteria (TSC) for specific control wording. Functional intersects with Untrassworthy Disclosure PRI-D.6.4 complaints, concerns or questions from authenticated data subjects about how the Services Criteria (TSC) for specific control wording. Functional intersects with Untrassworthy Disclosure PRI-D.6.4 complaints, concerns or questions from authenticated data subjects about how the Services Criteria (TSC) for specific control wording. Functional intersects with Untrassworthy Disclosure PRI-D.6.4 complaints, concerns or questions from authenticated data subjects about how the Services Criteria (TSC) for specific control wording. Functional intersects with Untrassworthy Disclosure PRI-D.6.4 complaints, concerns or questions from authenticated data subjects about how the Services Criteria (TSC) for specific control wording. Functional intersects with Untrassworthy Disclosure PRI-D.6.4 complaints, concerns or questions from authenticated data subjects about how the Services Criteria (TSC) for specific control wording. Functional intersects with Untrassworthy Disclosure PRI-D.6.4 complaints, concerns or questions from authenticated data subjects about how the Services Criteria (TSC) for specific control wording. Functional intersects with Untrassworthy Disclosure PRI-D.6.4 complaints, concerns or questions from authenticated or examination concerns or questions from authenticate	P5.1-POF3	Access to Their Personal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		PRI-06	(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the further, size or separes of providing access would be disproportionate to the benefit offered to the data subject through granting access; [2] Obtain answers on the specifics of how their PD is collected, enclosed, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD date to inaccuracies; (6) Request correction to their PD and (7) Restrict the further collecting, receiving, processing, storing, transmitting,	5	
Provides Understandable Reject Unauthenticated of Reject Unauthenticated of PROVIDE Unauthenticated of Reject Unauthenticated, or untrustworthy, disclosure requests.	P5.1-POF4	Personal Information Within Reasonable Time	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management	PRI-06.4	complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or	5	
Within Resonable Time Requests	P5.1-POF4	Provides Understandable Personal Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Untrustworthy Disclosure	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	5	



Secure Controls Framework (SCF) 35 of 4

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
P5.1-POF5	Informs Data Subjects If Access Is Denied [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or	5	
P5.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Updating & Correcting Personal Data (PD)	DCH-22.1	discoses of their Personal Data (PD). Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	5	
P5.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Correcting Inaccurate Personal Data	PRI-06.1	Mechanisms exist to establish and implement a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and [2) Disseminating corrections or amendments of PD to other authorized users of the	5	
P5.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Notice of Correction or Processing Change	PRI-06.2	PD. Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected or amended.	5	
P5.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	5	
P5.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or transmits, where the processes of the processes	5	
P5.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Updating Personal Data (PD)	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	
P5.2-POF1	Responds to Data Controller Requests [P]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or discoses of their Personal Data (PD).	5	
P5.2-POF1	Responds to Data Controller Requests [P]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	5	
P5.2-POF2	Communicates Denial of Access Requests [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Correcting Inaccurate Personal Data	PRI-06.1	Mechanisms exist to establish and implement a process for: (1) tats subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.	5	
P5.2-POF2	Communicates Denial of Access Requests [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
P5.2-POF2	Communicates Denial of Access Requests [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Updating Personal Data (PD)	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	
P5.2-POF3	Permits Data Subjects to Update or Correct Personal Information IPICI Permits Data Subjects to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
P5.2-POF3	Permits Data Subjects to Update or Correct Personal Information [PIIC1] Permits Data Subjects to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposace of their Personal Data (PD).	5	
P5.2-POF3	Permits Data Subjects to Update or Correct Personal Information IPIIC1	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	5	
P5.2-POF4	Communicates Denial of Correction Requests [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	
P6.0	Privacy Criteria Related to Disclosure and Notification	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know. Mechanisms exist to disclose Personal Data (PD) to third-parties only for the	10	
P6.1	N/A Communicates Privacy	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Information Sharing With Third Parties	PRI-07	purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject. Mechanisms exist to disclose Personal Data (PD) to third-parties only for the	5	
P6.1-POF1	Policies to Third Parties [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Information Sharing With Third Parties Data Privacy	PRI-07	purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject. Mechanisms exist to include data privacy requirements in contracts and other	5	
P6.1-POF1	Communicates Privacy Policies to Third Parties [P][C] Discloses Personal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Requirements for Contractors & Service Providers	PRI-07.1	acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
P6.1-POF2	Information Only When Appropriate [PIIC] Discloses Personal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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. Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties	5	
P6.1-POF2	Information Only When Appropriate [PI[C] Discloses Personal Information Only to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Limiting Personal Data (PD) Disclosures	PRI-01.7	for the sole purpose for which the PD was obtained. Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized	5	
P6.1-POF3	Appropriate Third Parties IPIIC1 Discloses Personal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Disclosure of Information	DCH-03.1	parties with a need to know. Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties	5	
P6.1-POF3	Information Only to Appropriate Third Parties IPIICI	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Limiting Personal Data (PD) Disclosures	PRI-01.7	for the sole purpose for which the PD was obtained.	5	
P6.1-POF4	Discloses Information to Third Parties for New Discloses Information to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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. Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties	5	
P6.1-P0F4	Third Parties for New Purposes and Uses [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Limiting Personal Data (PD) Disclosures	PRI-01.7	for the sole purpose for which the PD was obtained. Mechanisms exist to provide data subjects with an accounting of disclosures of their	5	
P6.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Accounting of Disclosures	PRI-14.1	Personal Data (PD) controlled by: (1) The organization; and/or IZI Relevant third-parties that their PD was shared with. Mechanisms exist to provide data subjects with an accounting of disclosures of their	5	
P6.2-POF1	Creates and Retains Record of Authorized Disclosures [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Accounting of Disclosures	PRI-14.1	Personal Data (PD) controlled by: (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.	10	
P6.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations. Mechanisms exist to timely-report incidents to applicable:	5	
P6.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	(1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
P6.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive /regulated data spills. Mechanisms exist to provide data subjects with an accounting of disclosures of their	5	
P6.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Accounting of Disclosures	PRI-14.1	Personal Data (PD) controlled by: (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.	5	
P6.3-POF1	Creates and Retains Record of Detected or Reported Unauthorized Disclosures [P] [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by: (1) The organization; and/or 2) Relevant third-parties that their PD was shared with.	10	
P6.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	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.	10	
P6.4-POF1	Evaluates Third-Party Compliance With Privacy Commitments (PIIC)	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
P6.4-POF1	Evaluates Third-Party Compliance With Privacy Commitments (PIIC)	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Limiting Personal Data (PD) 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	
P6.4-POF2	Commitments IPIIC1 Remediates Misuse of Personal Information by a Third Party IPIIC1	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 (PIIC)	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
P6.4-POF2	Remediates Misuse of Personal Information by a Third Party [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	



Secure Controls Framework (SCF) 36 of 4

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
P6.4-POF3	Obtains Commitments to Report Unauthorized Disclosures [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
P6.4-POF3	Obtains Commitments to Report Unauthorized Disclosures [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
P6.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
P6.5-POF1	Remediates Misuse of Personal Information by a Third Party IPIIC1	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 (PIIC)	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
P6.5-POF1	Remediates Misuse of Personal Information by a Third Party [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
P6.5-POF2	Reports Actual or Suspected Unauthorized Disclosures [PIIC]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 [PIIC1	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
P6.5-POF2	Reports Actual or Suspected Unauthorized Disclosures [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	5	
P6.6	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
P6.6-POF1	Identifies Reporting Requirements [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
P6.6-POF1	Identifies Reporting Requirements [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
P6.6-POF1	Identifies Reporting Requirements [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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, regulations and contractual obligations.	10	
P6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	5	
P6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and	5	
P6.7-POF1	Responds to Data Controller Requests [P]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Purpose Specification	PRI-02.1	(3) Regulatory authorities. Mechanisms exist to ensure the data privacy notice identifies the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted,	5	
P6.7-POF1	Responds to Data	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authority To Collect, Process, Store & Share	PRI-04.1	shared Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, update and/or share	5	
10.71011	Controller Requests [P]	Some and As a management of the specime control to any	Tunctional	maracata war	Personal Data (PD)	110-04.1	Personal Data (PD), either generally or in support of a specific business process. Mechanisms exist to define business processes with consideration for cybersecurity	,	
P6.7-POF1	Responds to Data Controller Requests [P]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and	5	
	Controller Requests (F)				Delinition		(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.		
P6.7-POF2	Identifies Types of Personal Information and Handling Process [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or	. 5	
P6.7-POF2	Identifies Types of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Portability	PRI-06.6	disposes of their Personal Data (PD). Mechanisms exist to format exports of Personal Data (PD) in a structured, machine-readable format that allows data subjects to transfer their PD to another controller	5	
	Handling Process [P][C] Identifies Types of				Personal Data (PD)		without hindrance. Mechanisms exist to export a data subject's available Personal Data (PD) in a readily		
P6.7-POF2	Personal Information and Handling Process [PIIC] Captures, Identifies, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Exports Data Subject	PRI-06.7	usable format, upon an authenticated request. Mechanisms exist to craft disclosures and communications to data subjects in a	5	
P6.7-POF3	Communicates Requests for Information [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Communications	PRI-17	manner that is concise, unambiguous and understandable by a reasonable person. Mechanisms exist to receive and process data controller communications pertaining	5	
P6.7-POF3	Captures, Identifies, and Communicates Requests for Information [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Controller Communications	PRI-18	rectnainsms was to receive and process data controller communications pertaining to: (1) Receiving and responding to data subject requests; (2) Updating/correcting Personal Data (PD); (3) Accounting for disclosures of PD; and	5	
							(a) Accounting for Discussives of PD; and (d) Accounting for PD that is stored, processed and/or transmitted on behalf of the data controller. Mechanisms exist to manage the quality, utility, objectivity, integrity and impact		
P7.0	Privacy Criteria Related to Quality	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Quality Management	PRI-10	determination and de-identification of sensitive/regulated data across the information lifecycle. Mechanisms exist to manage the quality, utility, objectivity, integrity and impact	5	
P7.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Quality Management	PRI-10	determination and de-identification of sensitive/regulated data across the information lifecycle.	5	
P7.1-POF1	Ensures Accuracy and Completeness of Personal Information [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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-POF2	Ensures Relevance of Personal Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 later mention if forced a	5	
P8.0	[P][C] Privacy Criteria Related to Monitoring and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Testing, Training & Monitoring	PRI-08	Information lifecycle. Mechanisms exist to conduct cybersecurity and data protection testing, training and monitoring activities	5	
P8.1	Enforcement N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or	. 5	
P8.1-POF1	Communicates to Data Subjects or Data Controllers [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Feedback Management	PRI-06.4	discoses of their Personal Data (PD). Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or	5	
P8.1-POF2	Addresses Inquiries,	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Feedback Management	PRI-06.4	discoses of their Personal Data (PD). Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or	5	
P8.1-POF3	Documents and Communicates Dispute Resolution and Recourse	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Feedback Management	PRI-06.4	disnoses of their Personal Data (PD). Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or	5	
P8.1-POF4	[P][C] Documents and Reports Compliance Review Results [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Documenting Data Processing Activities	PRI-14	disnoses of their Personal Data (PD). Mechanisms exist to document Personal Data (PD) processing activities that cover collecting, receiving, processing, storing, transmitting, updating, sharing and disposal actions with sufficient detail to demonstrate conformity with applicable	5	<u> </u>
P8.1-POF5	Documents and Reports Instances of Noncompliance [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Documenting Data Processing Activities	PRI-14	statutorv. regulatorv and contractual requirements. Mechanisms exist to document Personal Data (PD) processing activities that cover collecting, receiving, processing, storing, transmitting, updating, sharing and disposal actions with sufficient detail to demonstrate conformity with applicable	5	
P8.1-POF6	Performs Ongoing Monitoring [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Testing, Training & Monitoring	PRI-08	statutorv. regulatorv and contractual requirements. Mechanisms exist to conduct cybersecurity and data protection testing, training and monitoring activities	5	
	Horitoning [P][C]	<u> </u>		<u> </u>	i-ionitoring		I	1	



Secure Controls Framework (SCF) 37 of 40

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
PI1.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	5	
PI1.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	standards to achieve the specific goals of the process area. Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and other organizations; and other organizations; and other organizations; are received to the processes and reviews the processes as necessary, until an achievable set of protection needs is	5	
PI1.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	obtained. Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or/Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
PI1.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
PI1.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
PI1.1-POF1	Identifies Functional and Nonfunctional Requirements and Information Specifications	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
PH.1-POF1	Identifies Functional and Nonfunctional Requirements and Information Specifications	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and CJ information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is oritization.	5	
P11.1-POF1	Identifies Functional and Nonfunctional Requirements and Information Specifications	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production or Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle SDLC) bit. (1) Improve functionality (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
PI1.1-POF1	Identifies Functional and Nonfunctional Requirements and Information Specifications	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Vable Product (MPV) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
P11.1-P0F2	Defines Data Necessary to Support a Product or Service	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing criticality analysis for critical Technology Assets, Applications and/or Sorvices (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
P11.1-PDF2	Defines Data Necessary to Support a Product or Service	Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to procestlvely govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) io: (1) Improve functionality; (2) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
PII.1+POF2	Defines Data Necessary to Support a Product or Service	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Minimum Viable Product (PVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAS) in such a way that risk-based technical and functional specifications entire Minimum Valsier Product (PMP) critical establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
PI1.1-POF3	Defines Information Necessary to Support the Use of a Good or Product	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a critically analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
PI1.1-POF3	Defines Information Necessary to Support the Use of a Good or Product	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:	5	
PI1.1-POF3	Defines Information Necessary to Support the Use of a Good or Product	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAXS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
PI1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
PI1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software Development Practices	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
PI1.2-POF1	Defines Characteristics of Processing Inputs	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software Development Practices	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP)	5	
PI1.2-POF1	Defines Characteristics of Processing Inputs	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
PI1.2-POF2	Evaluates Processing Inputs Evaluates Processing	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software Development Practices	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP). Mechanisms exist to check the validity of information inputs.	5	
PI1.2-POF2 PI1.2-POF3	Inputs Creates and Maintains	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Input Data Validation Secure Software	TDA-18 TDA-06	Mechanisms exist to develop applications based on Secure Software Development	5	
P11.2-POF3	Records of System Inputs	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Development Practices	1DA-06	Practices (SSDP).	5	



Secure Controls Framework (SCF) 38 of

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
PI1.2-POF3	Creates and Maintains Records of System Inputs	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	(optional) 5	
PI1.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	10	
PI1.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Secure Software	TDA-06	business needs. Mechanisms exist to develop applications based on Secure Software Development	10	
		-			Development Practices Service Delivery		Practices (SSIP) Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning,		
PI1.3-POF1	Defines Processing Specifications	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(Business Process Support)	OPS-03	delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized	5	
							standards to achieve the specific goals of the process area. Mechanisms exist to define business processes with consideration for cybersecurity		
PI1.3-POF1	Defines Processing	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process	PRM-06	and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and	5	
FILSFORT	Specifications	DOWNLOAD AIGHA'S THIS SERVICES CITICATA (13G) for specific control wording.	runctional	litter sects with	Definition	FRINO	organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is	3	
PI1.3-POF1	Defines Processing	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software	TDA-06	nhtained Mechanisms exist to develop applications based on Secure Software Development	5	
FILSFORT	Specifications	DOWNLOAD ATOMS THUS SERVICES CITIENTS (1907) FOR SPECIAL CONTROL WORKING.	Pulicional	litter sects with	Development Practices	IDA-00	Practices (SSDP) Mechanisms exist to define supporting business processes and implement		
PI1.3-POF2	Defines Processing Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	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	5	
					оарропу		standards to achieve the specific goals of the process area. Mechanisms exist to define business processes with consideration for cybersecurity		
	Defines Processing				Business Process		and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other		
PI1.3-POF2	Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Definition	PRM-06	organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is	5	
PI1.3-POF2	Defines Processing	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software	TDA-06	Anhtained Mechanisms exist to develop applications based on Secure Software Development	5	
PII.3-POF2	Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Development Practices	TDA-06	Practices (SSDP) Mechanisms exist to define supporting business processes and implement		
PI1.3-POF3	Detects and Corrects Processing or Production Activity Errors	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting	5	
	ACTIVITY ETIOIS				Заррогі		business functions, workforce, and/or customers based on industry-recognized standards to achieve the seecific goals of the process area. Mechanisms exist to define business processes with consideration for cybersecurity		
	Detects and Corrects				Business Process		and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other		
PI1.3-POF3	Processing or Production Activity Errors	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Definition	PRM-06	organizations; and (2) Information protection needs arising from the defined business processes and	5	
	Detects and Corrects				Secure Software		revises the processes as necessary, until an achievable set of protection needs is obtained. Mechanisms exist to develop applications based on Secure Software Development		
PI1.3-POF3	Processing or Production	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Development Practices	TDA-06	Practices (ISSDP). Mechanisms exist to define supporting business processes and implement	5	
PI1.3-POF4	Records System Processing Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Service Delivery (Business Process	OPS-03	appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting	5	
					Support)		business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.		
							Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other		
PI1.3-POF4	Records System Processing Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	organizations; and (2) Information protection needs arising from the defined business processes and	5	
							revises the processes as necessary, until an achievable set of protection needs is obtained		
PI1.3-POF4	Records System Processing Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software Development Practices	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practines (SSDP) Mechanisms exist to define supporting business processes and implement	5	
PI1.3-POF5	Processes Inputs	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Service Delivery (Business Process	OPS-03	appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting	5	
	, , ,				Support)		business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.		
							Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines:		
PI1.3-POF5	Processes Inputs	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and	5	
							revises the processes as necessary, until an achievable set of protection needs is obtained		
PI1.3-POF5	Processes Inputs	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software Development Practices	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (ISSDP)	5	
							Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred;		
PI1.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Content of Event Logs	MON-03	(2) When (date and time) the event occurred; (3) Where the event occurred;	5	
							(4) The source of the event; (5) The outcome (success or failure) of the event; and		
							(6) The identity of any user/subject associated with the event.		
PI1.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion. Physical security mechanisms exist to restrict access to printers and other system	5	
PI1.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Access Control for Output Devices	PES-12.2	output devices to prevent unauthorized individuals from obtaining the output.	5	
PI1.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software Development Practices	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
PI1.4-POF1	Protects Output	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls. Mechanisms exist to define supporting business processes and implement	5	
PI1.4-POF1	Protects Output	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Service Delivery (Business Process	OPS-03	appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting	5	
					Support)		business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.		
							Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other		
PI1.4-POF1	Protects Output	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	organizations; and (2) Information protection needs arising from the defined business processes and	5	
							revises the processes as necessary, until an achievable set of protection needs is obtained		
PI1.4-POF1	Protects Output	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software Development Practices	TDA-06	Mechanisms exist to develop applications based on Secure Software Development <u>Practices ISSDP</u> . Mechanisms exist to facilitate the implementation of data protection controls.	5	
PI1.4-POF2	Intended Parties	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls. Mechanisms exist to define supporting business processes and implement	5	
PI1.4-POF2	Distributes Output Only to Intended Parties	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Service Delivery (Business Process	OPS-03	appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting	5	
					Support)		business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area Mechanisms exist to define business processes with consideration for cybersecurity		
							Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other		
PI1.4-POF2	Distributes Output Only to Intended Parties	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	(2) Information protection needs arising from the defined business processes and	5	
	Distribut 2				0 0.1		revises the processes as necessary, until an achievable set of protection needs is obtained.		
PI1.4-POF2	Distributes Output Only to Intended Parties Distributes Output	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software Development Practices	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP) Mechanisms exist to facilitate the implementation of data protection controls.	5	
PI1.4-POF3	Completely and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to define supporting business processes and implement	5	
PI1.4-POF3	Distributes Output Completely and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Service Delivery (Business Process	OPS-03	appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting	5	
	Accurately				Support)		business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area. Machanisms exist to define business processes with consideration for othersecurible.		
	Distributes Output						Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other		
PI1.4-POF3	Completely and Accurately	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and	5	
							revises the processes as necessary, until an achievable set of protection needs is obtained		



Secure Controls Framework (SCF) 39 of 4

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF#	Secure Controls Framework (SCF)	Strength of Relationship	Notes (optional)
	Distributes Output		Rationale	Relationship	Secure Software		Control Description Mechanisms exist to develop applications based on Secure Software Development	(optional)	
PI1.4-POF3	Completely and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Development Practices	TDA-06	Practices (SSDP)	5	
PI1.4-POF4	Creates and Maintains Records of System Output	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
PI1.4-POF4	Creates and Maintains Records of System Output Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 saccelific coals of the process area.	5	
PI1.4-POF4	Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is intrinsional.	5	
PI1.4-POF4	Creates and Maintains Records of System Output	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software Development Practices	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP)	5	
PI1.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
PI1.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
PI1.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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	
PI1.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software	TDA-06	Mechanisms exist to develop applications based on Secure Software Development	5	
PI1.5-POF1	Protects Stored Items	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Development Practices Data Protection	DCH-01	Practices (SSDP). Mechanisms exist to facilitate the implementation of data protection controls.	5	
PI1.5-POF1	Protects Stored Items	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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, worldroce, and/or customers based on industry-recognized standards to achieve the sociefic social of the process area.	5	
PI1.5-POF1	Protects Stored Items	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is offered and achievable set.	5	
PI1.5-POF1	Protects Stored Items	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software Development Practices	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
PI1.5-POF2	Archives and Protects	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
PI1.5-POF2	Archives and Protects System Records	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 secretic socials of the process area.	5	
PI1.5-POF2	Archives and Protects System Records	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for ophersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and organizations; and of the organizations; and organizations; and organizations; and organizations are resulted to the organizations of the organizations and organizations are resulted to the organization of the organizat	5	
PI1.5-POF2	Archives and Protects System Records	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software Development Practices	TDA-06	Mechanisms exist to develop applications based on Secure Software Development	5	
PI1.5-POF3	Stores Data Completely and Accurately	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection	DCH-01	Practices (SSDP) Mechanisms exist to facilitate the implementation of data protection controls.	5	
PI1.5-POF3	Stores Data Completely and Accurately	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 societic social of the process area.	5	
PI1.5-POF3	Stores Data Completely and Accurately	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is of infrained.	5	
PI1.5-POF3	Stores Data Completely and Accurately	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software Development Practices	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP)	5	
PI1.5-POF4	Creates and Maintains Records of System	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
PI1.5-POF4	Creates and Maintains Records of System Storage Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	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 sacefile costs of the process area.	5	
PI1.5-POF4	Creates and Maintains Records of System Storage Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is	5	
PI1.5-POF4	Creates and Maintains	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software	TDA-06	Obtained. Mechanisms exist to develop applications based on Secure Software Development	5	
	Records of System				Development Practices		Practices (SSDP).	-	



Secure Controls Framework (SCF) 40 of 4