Set Theory Relationship Mapping (STRM)

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2025. 2
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document:
Focal Document URL:
Published STRM URL:
https://www.acpo.org/interestreas/fr/d/assuranceadvisoryservices/aicposoc2report.html
https://securecontrolsframework.com/content/strm/scf-strm-general-aicpa-toc-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 (ontional)	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 systems that are susceptible to	5	
A1.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Capacity Planning	CAP-03		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		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	casacity requirements. Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical systems, applications and services.	10	
A1.1-POF2	Forecasts Capacity	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Capacity Planning	CAP-03		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	during contingency operations. 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	BCD-01	canacity requirements. Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan	10	
A1.2	NA	DOWNLOAD ACE AS THAT SERVICES CIRCING (ISO) TO SPECIAL COURTS WORKING.	Functional	Subset of	(BCMS)	BCD-01	(COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks). Mechanisms exist to establish an alternate storage site that includes both the assets	10	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Alternate Storage Site Separation from Primary	BCD-08	and necessary agreements to permit the storage and recovery of system backup information. Mechanisms exist to separate the alternate storage site from the primary storage site	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Site	BCD-08.	to reduce susceptibility to similar threats. Mechanisms exist to identify and mitigate potential accessibility problems to the	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Accessibility	BCD-08.:	Mechanisms exist to establish an alternate processing site that provides security	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Alternate Processing Site Separation from Primary	BCD-09	Mechanisms exist to separate the alternate processing site from the primary	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Site	BCD-09.	processing site to reduce susceptibility to similar threats. Mechanisms exist to identify and mitigate potential accessibility problems to the	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Accessibility	BCD-09.	atternate processing site and possible mitigation actions, in the event of an area- wide disruption or disaster. Mechanisms exist to address priority-of-service provisions in alternate processing	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.		5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Telecommunications Services Availability Telecommunications	BCD-10		5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Priority of Service Provisions	BCD-10.	1 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	the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point	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.	Objectives (RPOs). Mechanisms exist to routinely test backups that verify the reliability of the backup rocess, 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.:	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.	Mechanisms exist to reimage assets from configuration-controlled and integrity-	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cryptographic Protection	BCD-11.	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	Information System Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of systems to a known state after a disruption, compromise or failure.	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Transaction Recovery	BCD-12.	Mechanisms exist to utilize specialized backup mechanisms that will allow 1 transaction recovery for transaction-based applications and services 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.	Mechanisms exist to implement real-time or near-real-time failover capability to	5	
A1.2	N/A	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	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: (1) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate said and easy access for personnet; 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 primary power source.	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Emergency Lighting	PES-07.4	Facility security mechanisms exist to utilize and maintain automatic emergency	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	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		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	,	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		5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Temperature & Humidity Controls	PES-09	emergency responders. Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Monitoring with Alarms /	PES-09.1	Facility security mechanisms exist to trigger an alarm or notification of temperature	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Alternate Work Site	PES-11	access. Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection Information Leakage Due To Electromagnetic	PES-13	minimize the opportunity for unauthorized access. Facility security mechanisms exist to protect the system from information leakage	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Signals Emanations Electromagnetic Pulse	PES-15	Physical security mechanisms exist to employ safeguards against Electromagnetic Pulse (EMP) damage for systems and system components.	5	
A1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(EMP) Protection	RSK-03	Pulse (EMP) damage for systems and system components. Mechanisms exist to identify and document risks, both internal and external.	5	
71.4		and the state of t	cuolidi	wood with	· · · · · · · · · · · · · · · · · · ·	03	1	Ŭ	



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 (ontional)	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 systems and data.	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	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
A1.2-POF1	Identifies Environmental Threats	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-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 assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	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	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	Monitoring with Alarms / Notifications	PES-09.1	and humidity changes that be potentially harmful to personnel or equipment.	5	
A1.2-POF3	Implements and Maintains Environmental Protection Mechanisms	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 assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
A1.2-POF3	Implements and Maintains Environmental Protection Mechanisms	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	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
A1.2-POF4	Implements Alerts to Analyze Anomalies	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.	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	Facility security mechanisms exist to trigger an alarm or notification of temperature and humidity changes that be potentially harmful to personnel or equipment.	5	
A1.2-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 assets and services (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 & data privacy- related incidents. Mechanisms exist to cover the preparation, automated detection or intake of	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	incident reporting, analysis, containment, eradication and recovery.	5	
A1.2-POF5	Responds to 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-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 assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	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-01.2	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	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	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 satisfying 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	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 capable of meeting both 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	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 assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	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	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 assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	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	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constrains facting 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	
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 Data	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	Tests Integrity and Completeness of Backup Data	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	Tests Integrity and	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.	5	



Secure Controls Framework (SCF) 2 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)
C1.1	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.	(optional) 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	Apprivative statutory, regulatory and contractual requirements. 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: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purposely 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 (2) liseo organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived 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.	10	
C1.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security	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	incidents and to meet statutury, regulatory and contractual retention requirements. Mechanisms exist to: (I) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purposeigl identified in the notice or as required by law; (2) bipose of, detroys, exists, and/or enorymites the Po, regulates of the (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originata, 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 Person 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) lispose of, detroys, earses, and/or anonymizes the Po, regardless of the method of storage, and (3) the organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originats, copies and archived records).	5	
C1.2-POF2	Destroys Confidential	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	Information 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	5	
	Information Destroys Confidential						formal procedures. Mechanisms exist to sanitize system media with the strength and integrity		
C1.2-POF2	Information	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 disposal, release out of organizational control or release for reuse.	5	
C1.2-POF2	Destroys Confidential Information	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. Mechanisms exist to:	5	
C1.2-POF2	Destroys Confidential Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Personal Data (PD) Retention & Disposal	PRI-05	(1) Retain Personal Data (PD), including metadats, for an organization-defined time period to halffill the purpose(s) identified in the notice or as required by law; (2) Dispose of, districtly, crases, and/or anonymizes the PD, regardless of the metador of the metador of the control of PD (including originals, copies and archived 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	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
CC1.1	COSO Principle 1	Download AlCPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Program Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
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 enterorise-wide cybersecurity & 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 & data privacy 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-P0F1	Sets the Tone at the Top	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Cybersecurity & Data Protection Governance		reasonable assurance that a policy has been violated. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
CC1.1-POF1	Sets the Tone at the Top	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Program Business As Usual (BAU)	GOV-14	Mechanisms exist to incorporate cybersecurity & data privacy principles into 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	Secure Practices Human Resources Security Management	HRS-01	Business As Usual (BAU) practices through executive leadership involvement. Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.1-POF2	Establishes Standards of	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	
	Conduct Evaluates Adherence to						use of technologies, including consequences for unacceptable behavior. Mechanisms exist to develop, report and monitor cybersecurity & data privacy		
CC1.1-POF3	Standards of Conduct Evaluates Adherence to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Measures of Performance Cybersecurity & Data	GOV-05	program measures of performance. Mechanisms exist to provide a cybersecurity & data protection controls oversight	10	
CC1.1-POF3	Evaluates Adherence to Standards of Conduct Evaluates Adherence to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Protection Controls Oversight Cybersecurity & Data	CPL-02	function that reports to the organization's executive leadership. Mechanisms exist to regularly review processes and documented procedures to	10	
CC1.1-POF3	Standards of Conduct Evaluates Adherence to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection Assessments	CPL-03	ensure conformity with the organization's cybersecurity & data protection policies, standards and other applicable requirements.	5	
CC1.1-POF3	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. Mechanisms exist to document and review instances of non-compliance with	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 mitiration 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	mitigation 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	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	Commitment Considers Contractors and Vendor Employees in Demonstrating Its Commitment	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 the services and product supply chains; and (2) Take appropriate remediation actions to minimize the optionization's exposure to	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	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
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	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESP).	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	Third-Party Personnel Security	TPM-06	staxenotoers and external service Providers (ESP3). Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
L	Commitment	1	1		1	1	1		L



cure Controls Framework (SCF) 3 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)
CC1.2	COSO Principle 2	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Governance	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
CC1.2	COSO Principle 2	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Program 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 & data privacy program measures of performance.	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	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 & data privacy program. Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the	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 & data privacy 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 recular 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 & 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	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	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	
CC1.2-POF1	Establishes Oversight Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defining Business Context & Mission	GOV-08	managing data and technology-related risks. 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	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	oositions. 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	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	
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 recular basis.	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	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 ossitions.	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 basis.	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 & 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 and managing data and technology-related risks.	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	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 & data privacy 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	
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 regular 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 manacing data and technology-related risks. Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
CC1.3-POF3	Defines, Assigns, and Limits Authorities and Responsibilities	Download AICPA's Trust Services Criteria (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 result hasis.	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	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring	5	
CC1.3-POF3	Responsibilities Defines, Assigns, and Limits Authorities and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authoritative Chain of Command	GOV-04.2		5	
	Responsibilities	I		l		L	managing data and technology-related risks.	l	



Secure Controls Framework (SCF) 4 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)
CC1.3-POF3	Defines, Assigns, and Limits Authorities and Responsibilities	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-POF3	Defines, Assigns, and Limits 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 & data privacy 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	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	5	
CC1.3-POF4	Responsibilities 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	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 & data privacy controls between internal	5	
CC1.3-POF5	Responsibilities N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(RASCI) Matrix Stakeholder Accountability Structure	GOV-04.1	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	
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	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 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 (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
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	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-POF6	Establishes Structures, Reporting Lines, and 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	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-POF6	Establishes Structures, Reporting Lines, and Authorities to Support	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	Establishes Structures, Reporting Lines, and Authorities to Support Establishes Structures,	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 impressed launifully fairly and transparantly Mechanisms exist to ensure that the interests of external service providers are	5	
CC1.3-POF6	Reporting Lines, and Authorities to Sunnort COSO Principle 4	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	Conflict of Interests Human Resources	TPM-04.3 HRS-01	consistent with and reflect organizational interests. Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC1.4	COSO Principle 4	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security Management Cybersecurity & Data Privacy Resource	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity & data privacy programs and	5	
CC1.4	COSO Principle 4	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management Allocation of Resources	PRM-03	document all exceedions to this requirement. 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 Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
CC1.4	COSO Principle 4	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Continuing Professional Education (CPE) - Cybersecurity & Data	SAT-03.7	Mechanisms exist to ensure cybersecurity & data privacy personnel receive Continuing Professional Education (CPE) training to maintain currency and proficiency with industry-recognized secure practices that are pertinent to their	5	
CC1.4-POF1	Establishes Policies and Practices	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Privacy Personnel Publishing Cybersecurity & Data Protection Documentation	GOV-02	assigned roles and responsibilities. Mechanisms exist to establish, maintain and disseminate cybersecurity & 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. Mechanisms exist to ensure policies, processes, procedures and practices related to	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	the mapping, measuring and managing of Artificial Intelligence (AI) 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 (Al) and Autonomous Technologies (AAT)-related operator and practitioner proficiency requirements for Artificial Intelligence (Al) and Autonomous Technologies (AAT) are defined, assessed and documented.	5	
CC1.4-POF2	Evaluates Competence and Addresses Shortcomings Evaluates Competence	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. Mechanisms exist to identify newty onboarded personnel for enhanced monitoring	5	
CC1.4-POF2	and Addresses Shortcomings	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. Mechanisms exist to ensure that all security-related positions are staffed by	5	
CC1.4-POF2	Evaluates Competence and Addresses Shortcomings	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Competency Requirements for Security- Related Positions	HRS-03.2	qualified individuals who have the necessary skill set.	5	
CC1.4-POF2	Evaluates Competence and Addresses Shortcomings Evaluates Competence	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identify Critical Skills & Gaps	HRS-13	Mechanisms exist to evaluate the critical cybersecurity & data privacy skills needed to support the organization's mission and identify gaps that exist. Mechanisms exist to facilitate the implementation of third-party management	5	
CC1.4-POF2	and Addresses Shortcomings Evaluates Competence	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	controls. Mechanisms exist to monitor, regularly review and assess External Service Providers	5	
CC1.4-POF2	and Addresses Shortcomings	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Review of Third-Party Services Robust Stakeholder	TPM-08	(ESPs) for compliance with established contractual requirements for cybersecurity & data orivacy controls. Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence	5	
CC1.4-POF3	Attracts, Develops, and Retains Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Engagement for AI & Autonomous Technologies	AAT-11	(Al) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts. Mechanisms exist to ensure Artificial Intelligence (Al) and Autonomous Technologies	5	
CC1.4-POF3	Attracts, Develops, and Retains Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Al & Autonomous Technologies Stakeholder Diversity	AAT-13	(AAT) stakeholder competencies, skills and capacities incorporate demographic diversity, broad domain and user experience expertise.	5	
CC1.4-POF3	Attracts, Develops, and Retains Individuals Attracts, Develops, 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. Mechanisms exist to identify newly onboarded personnel for enhanced monitoring	5	
CC1.4-POF3	Attracts, Develops, and Retains Individuals Attracts, Develops, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Probationary Periods Identify Critical Skills &	HRS-02.2	during their probationary period. Mechanisms exist to evaluate the critical cybersecurity & data privacy skills needed	5	
CC1.4-POF3	Retains Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Gaps	HRS-13	to support the organization's mission and identify gaps that exist. Mechanisms exist to facilitate the implementation of security workforce	5	
CC1.4-POF3	Attracts, Develops, and Retains Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Privacy-Minded Workforce Continuing Professional	SAT-01	development and awareness controls. Mechanisms exist to ensure cybersecurity & data privacy personnel receive	5	
CC1.4-POF3	Attracts, Develops, and Retains Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Education (CPE) - Cybersecurity & Data Privacy 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-POF3	Attracts, Develops, and Retains Individuals	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. Mechanisms exist to monitor, regularly review and assess External Service Providers	5	
CC1.4-POF3	Attracts, Develops, and Retains Individuals Plans and Prepares for	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 & data privacy controls.	5	
CC1.4-POF4 CC1.4-POF4	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 Functional	intersects with	Identify Critical Skills & Gaps Perform Succession	HRS-13 HRS-13.4	Mechanisms exist to evaluate the critical cybersecurity & data privacy skills needed to support the organization's mission and identify gaps that exist. Mechanisms exist to perform succession planning for vital cybersecurity & data	5	
CC1.4-POF5	Succession Considers the Background of Individuals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Planning Personnel Screening	HRS-04	privacy roles. 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	
L	Individuals	1	Î		,	1	1	i	



cure Controls Framework (SCF) 5 of 4

Columbia	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)
Column C	CC1.4-POF6	Competency of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Requirements for Security	HRS-03.2		10	
Product Services Product Ser	CC1.4-POF7	Maintain Technical	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Privacy Awareness	SAT-02		5	
Process Toronto Services Process Toronto Ser	CC1.4-POF7	Maintain Technical	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		SAT-03	training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and	5	
Process Description Desc	CC1.4-POF7	Maintain Technical	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Education (CPE) - Cybersecurity & Data	SAT-03.7	Mechanisms exist to ensure cybersecurity & data privacy personnel receive Continuing Professional Education (CPE) training to maintain currency and proficiency with industry-recognized secure practices that are pertinent to their	5	
Column	CC1.4-POF7	Maintain Technical	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Continuing Professional Education (CPE) - DevOps	SAT-03.8	Mechanisms exist to ensure application development and operations (DevOps) personnel receive Continuing Professional Education (CPE) training on Secure	5	
COLD COST	CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Measures of Performance	GOV-05	program measures of performance.	5	
COLD COORDINGS Owned 607% in the force contending for the party contend worthy Proceedings Cold	CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		GOV-05.1	to assist organizational management in performance monitoring and trend analysis of the cybersecurity & data privacy program.	5	
COLD COORDINGS CONTROLLS C	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	5	
Col.	CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant	5	
COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is brown Childs (TSC) to quarter control working. COLD COST-PRINGES Demonstrat ACPVA That is b	CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CPL-01.1	statutory, regulatory and/or contractual obligations to develop appropriate risk	5	
CC1.5 CODD Procepts Demonstrate Street Control Street Stre	CC1.5	COSO Principle 5	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	5	
Col. S. COLO Principals Developed MOVA's Trust Environ. Christon (PSC) for specific control wording. Processor in Col. Secti	CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Access Agreements	HRS-06		5	
CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise Center (TSC) for specific comits wanding. CC1.5 COSP Princips 5 Developed ACCPA's That Envise	CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	intersects with		HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar	5	
COLS DOOD Principals Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. COLS DOOD Principals Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. COLS DOOD Principals Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. COLS DOOD Principals Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. COLS DOOD Principals Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit ventring. Functional College Sounded ACPA's Trust Evokes Crimer (15) to specific commit								details, or both employees and third-parties.		
CCLS PROGRES Demonstratives for the Services Challed (SC) for specific corrors working. CCLS CCC Promogras 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS CCC Promogras 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS CCC CCC CCC Promogras 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS CCC Promogras 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS CCC Promogras 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS CCC Promogras 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS CCC Promogras 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS POTE 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS POTE 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS POTE 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS POTE 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS POTE 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS POTE 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS POTE 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS POTE 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS POTE 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS POTE 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS POTE 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS POTE 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS POTE 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS POTE 5 Demonstratives for the Services Challed (SC) for specific corrors working. CCLS POTE 5 Demonstratives for the Ser								oolicies, standards and procedures. Mechanisms exist to conduct employee misconduct investigations when there is		
CC1.5 COSD Principles								Mechanisms exist to adjust logical and physical access authorizations to systems		
CC1.5 COSO Principle 3 COSO Principle 4 COSO Principle 3 COSO Principle 4 COSO Principle 3 COSO Principle 4	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 COSO P	CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Asset Collection	HRS-09.1		5	
CC1.5 PCPI Entours Accountability Through Structures, Description of Part Services Criteria (TSC) for specific control wording. CC1.5-PCPI Entours Accountability Through Structures. Authorities, and Entours Accountability Through Structures. CC1.5-PCPI Through Structures. CC1.5-PCP	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	5	
Enforces Accountability in Trough Structures Authorities, and CC1.5-POP1 CC1.5-POP2 CC1.5-POP2 CC1.5-POP2 CC1.5-POP2 CC1.5-POP2 CC1.5-POP2 CC1.5-POP3 CC1.5-POP4 CC1.5-POP5 CC1.5-POP4 CC1.5-POP6 CC1.	CC1.5	COSO Principle 5	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		HRS-09.3	individuals of applicable, legally binding post-employment requirements for the	5	
Coll-POFI Trough Structures, Authorities, and Authorities, and Esponsibilities (Coll-POFI Esponsibilities) (Coll-P	CC1.5-POF1	Through Structures,	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring	5	
Entotices Accountability Through Structures, Authorities, and Entablishes Performance Measure, Incentives, and Responsibilities of all personnel. C1.5-PDF2 Entablishes Performance Responsibilities of all personnel. C1.5-PDF3 Measure, Incentives, and Responsibilities of all personnel. Entablishes Performance Responsibilities of Performance Responsibilities of Performance of Performance of Performance of Perform	CC1.5-POF1	Through Structures, Authorities, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		GOV-04.2	communication to remove ambiguity from individuals and teams related to	5	
CC1.5-POF2 Measures, Incentives, and Developed AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Measures, Incentives, and Developed AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Subset of Security Management Formance Intersects with Pressures Developed AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Program Oversight Functional Intersects with Pressures Developed AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Pressures Pressures Developed AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Program Oversight Functional Intersects with Pressures Pressures Developed AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Pressures Pressures Developed AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Pressures Pressures Developed AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Pressures Pressures Developed AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Pressures Pressures Pressures Developed AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Pressures Pressure	CC1.5-POF1	Enforces Accountability	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
CC1.5-POF2 Considers Excessive Pressures Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional subset of Program Oversight	CC1.5-POF2	Measures, Incentives, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Measures of Performance	GOV-05		5	
CC1.5-POF3 Measures, Incentives, an Developed in Composing Relevance Composition of Origining Relevance Considers Excessive Pressures	CC1.5-POF2	Measures, Incentives, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of		HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
Evaluates Performance Measures, Incentives, and Demonstrated Formance Resources Pressures CC1.5-POF4 CC1.5-POF4 CC1.5-POF4 CC1.5-POF5 Demonstrated Formance Pressures Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Functional Inte	CC1.5-POF3	Measures, Incentives, and Rewards for Ongoing Relevance	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		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	5	
CC1.5-POF4 Considers Excessive Pressures CC1.5-POF4 Considers Excessive Pressures CC1.5-POF5 Considers Excessive Excessive Excessive Pressures CC1.5-POF5 Considers Excessive Excessive Excessive Excessive Pressures CC1.5-POF5 Considers Excessive E	CC1.5-POF3	Evaluates Performance Measures, Incentives, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		HRS-01		5	
CC1.5-POF4 Considers Excessive Pressures Considers Excessive Pressures	CC1.5-POF4		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of		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	10	
CC1.5-POF5 and Rewards or Disciplines flowful but and AICPA's Trust Services Criteria (TSC) for specific control wording. Functional subset of Sterring Committee a divisory board, comprised of key Program Oversign t Evaluates Performance CC1.5-POF5 and Rewards or Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Measures of Performance S 004-61, applicable trusting to a specific control wording to the service of the service	CC1.5-POF4		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
Evaluates Performance CC1.5-POF5 and Rewards or Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Messures of Performance of Performance. Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	CC1.5-POF5	and Rewards or	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of		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	10	
	CC1.5-POF5		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 & data privacy program measures of performance.	5	
Evaluates Performance and Rewards or Discipline Individuals Discipline Individual Discipline Individual Discipline Individual Discipline Individual Discipline Individual Discipline Individual Discipline Ind	CC1.5-POF5	and Rewards or	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
Evaluates Performance and Rewards or Discipline Individuals Discipline Individual Discipline Individual Discipline Individual Discipline Individual Discipline Individual Discipline Individual Discipline Ind	CC1.5-POF5	and Rewards or	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Personnel Sanctions	HRS-07		5	
CC1.5-POF6 Takes Disciplinary Actions Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional equal Personnel Sanctions HRS-07 policies, standards and procedures.	CC1.5-POF6	Takes Disciplinary Actions	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Personnel Sanctions	HRS-07	policies, standards and procedures.	10	
CC2.1 COSO Principle 13 Download AICPA's Trust Services Oriteria (TSC) for specific control wording. Functional intersects with Functional intersects with Flow Diagrams & Data Flow Diagrams (DFDs) (3) Document all sensitive/regulated data flows.	CC2.1	COSO Principle 13	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		AST-04	Contain sufficient detail to assess the security of the network's architecture; Reflect the current architecture of the network environment; and	5	
CC2.1 COSO Principle 13 Download AICPA's Trust Services Oriteria (TSC) for specific control wording. Functional intersects with Data Protection DCH-01 Mechanisms exist to facilitate the implementation of data protection controls.	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 Data Stewardship Data Stewardship is assigned, documented and 5 communicated.	CC2.1	COSO Principle 13	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		DCH-01.1	communicated.	5	
CC2.1 COSO Principle 13 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Classification Classificatio	CC2.1	COSO Principle 13	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		DCH-02	applicable statutory, regulatory and contractual requirements.	5	
CC2.1 COSO Principle 13 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Data Quality Operations Deta Quality Operations The operation of information across the information infecycle.	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	5	
CC2.1 COSO Principle 13 Download AICPA's Trust Services Oriteria (TSC) for specific control wording. Functional intersects with intersects with Support) Download AICPA's Trust Services Oriteria (TSC) for specific control wording. Functional intersects with intersects with Support) Support) Mechanisms exist to define supporting business processes and implement support and service management to ensure appropriate generating. Support of the originations technology capabilities supporting 5 business functions, worderose, and/or customers based on industry-recognized extenders in consider the process area.	CC2.1	COSO Principle 13	Download AICPA's Trust Services Criteria (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	
CC2.1-POF1 Identifies Information Requirements Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Define Control Objectives GOV-99 implementation and management of the organization's internal control system. 5	CC2.1-POF1		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	*	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	
Identifies Information Operationalizing Mechanisms exist to compel data and/or process owners to operationalize	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 compet data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	



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 (optional)	Notes (optional)
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	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	GOV-15	standards to achieve the specific goals of the process area. Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service	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	Protection Practices Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	under their control. Mechanisms exist on 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 sencefile could set the recognized standards to achieve the sencefile could set the recognized.	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 & data privacy 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 specific soals 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	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 & data privacy program measures of performance. Mechanisms exist to define supporting business processes and implement	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	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	
CC2.1-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	(4) includes organization-defined information deemed necessary to achieve effective property accountability; and (5) is available for review and audit by designated organizational personnel.	5	
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 Confidentially, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
CC2.1-POF7	Classifies Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Data & Asset Classification	DCH-02		10	
CC2.1-POF7	Classifies Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Reclassification	DCH-11	Mechanisms exist to reclassify data, including associated systems, applications and services, commensurate with the security category and/or classification level of the information.	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	Mechanisms exist to determine cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties).	5	
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	Nechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services in use; (2) identifies authorized software products, including business justification details; (3) is at the level of granularity demand necessary for tracking and reporting; (4) includes organization-defined information deemed necessary to achieve effective property accountability, and (5) is available for review and audit by designated organizational personnel.	5	
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		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		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	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		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		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 control. Mechanisms exist to provide a cybersecurity & 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	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Measures of Performance Key Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance. Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs)	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	to assist organizational management in performance monitoring and trend analysis of the cybersecurity δ data privacy program.	5	



Secure Controls Framework (SCF) 7 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)
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Key Risk Indicators (KRIs)	GOV-06	Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the cybersecurity & data privacy program.	5	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Define Control Objectives	GOV-0	Mechanisms exist to establish control objectives as the basis for the selection,	5	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Defined Roles & Responsibilities	HRS-0		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-0	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	 ISOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks. Mechanisms exist to facilitate the implementation of cybersecurity & data privacy- 	5	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Privacy Portfolio Management	PRM-0	1 related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	5	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-0	at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
CC2.2	COSO Principle 14	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Engineering Principles	SEA-0	implementation and modification of systems and services.	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	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments. Mechanisms exist to establish, maintain and disseminate cybersecurity & 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-0		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-0	9 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-0	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	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material t the organization's cybersecurity & 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-0		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	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-0	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	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-0	Mechanisms exist to cover:	5	
CC2.2-POF4	Selects Relevant Method	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Steering Committee &	GOV-01	Automated exent detection or manual incident report intake: Mechanism exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key	5	
	of Communication Selects Relevant Method				Program Oversight		cybersecurity, data privacy and business executives, which meets formally and on a regular basis.		
CC2.2-POF4	of Communication	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Contacts With Authorities	GOV-0	enforcement and regulatory bodies. Mechanisms exist to establish contact with selected groups and associations within	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 Groups & Associations	GOV-0	the cybersecurity & data privacy communities to: (1) Facilitate organic cybersecurity & data privacy education and training for 7 organizational personnes; (2) Maintain currency with recommended cybersecurity & data privacy practices, techniques and technologies; and (3) Share current cybersecurity and/or data privacy-related information including threats uniformatilities and incidented.	5	
CC2.2-POF5	Communicates Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Defined Roles & Responsibilities	HRS-0	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	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs). Mechanisms exist to cover:	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-0	(1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (6) Endication: and	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	Integrated Security Incident Response Team (ISIRT)	IRO-0	.ffill Benomers Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
CC2.2-POF6	Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Situational Awareness For Incidents	IRO-0		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 Stakeholder Reporting	IRO-10	(3) Regulatory authorities.	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	Cyber Incident Reporting for Sensitive Data	IRO-10		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	Coordination With External Providers	IRO-11		5	
CC2.2-POF7	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-0	Mechanisms exist to establish, maintain and disseminate cybersecurity & data 2 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-0	occur to ensure their continuing suitability, adequacy and effectiveness.	5	
CC2.2-POF7	Communicates Objectives and Changes to Objectives	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Define Control Objectives	GOV-0	,	5	
CC2.2-POF8	Communicates Information to Improve	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Privacy-Minded Workforce	SAT-0	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
CC2.2-POF8	Communicates Information to Improve Security Knowledge and Awareness	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-0	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
CC2.2-POF8	Communicates Information to Improve Security Knowledge and Awareness	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cyber Threat Environment	SAT-03	Mechanisms exist to provide rote-based cybersecurity & data privacy awareness training that is current and relevant to the cyber threats that users might encounter is day-to-day business operations.	n 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	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03	Mechanisms exist to ensure that every user accessing a system processing, storing 3 or transmitting sensitive / regulated data is formally trained in data handling requirements.	5	
CC2.2-POF9	Communicates Information to Improve	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Privileged Users	SAT-03	Mechanisms exist to provide specific training for privileged users to ensure privilege	d 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	Responsible, Accountable, Supportive,	TPM-05	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to	5	
SSEZFOR	Privacy Knowledge and Awareness		, unctional	managets with	Consulted & Informed (RASCI) Matrix		4 delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	,	



Secure Controls Framework (SCF) 8 of 40

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 (optional)	Notes (optional)
Management Man	CC2.2-POF9	Information to Improve	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 & data privacy control assignments accurately reflect current	5	
Machine Mach	CC2 2 BOE0	Awareness Communicates	Download AICBA's Trust Sandoos Critario (TSC) for appoiling control wording	Eunstional	interposts with	Attack Surface Scene	VDM 01.1	Mechanisms exist to define and manage the scope for its attack surface		
		Privacy Knowledge and								
Column C			Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		GOV-08	organization's mission.	5	
Control Cont	CC2.2-POF10		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IRO-01	facilitate an organization-wide response capability for cybersecurity & data privacy- related incidents. Mechanisms exist to cover: (1) Preparation;	5	
	CC2.2-POF10		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	(3) Analysis; (4) Containment; (5) Eradication; and	5	
	CC2.2-POF10		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the	5	
Section Contraction Cont	CC2.2-POF10		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Plan	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident	5	
Columnition	CC2.2-POF11	Information About System		Functional	intersects with	Asset Scope Classification	AST-04.1	identifying, assigning and documenting the appropriate asset scope categorization	5	
COLUMN C	CC2.2-POF11	Information About System	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Boundary Graphical	AST-04.2	systems, applications, services and third parties by graphically representing applicable boundaries.	5	
CC2 2 PG 12 Communication and boundaries CC2 2 PG 12 Communication and boundar	CC2.2-POF11	Information About System		Functional	intersects with	Compliance Scope	CPL-01.2	privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
COC2 2FOT 12 Commissional Book and Section 1 and Section	CC2.2-POF11	Information About System	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Assessment Boundaries	IAO-01.1	boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the data and systems under review.	5	
CC2 2 POT 12 Communication System CC2 2	CC2.2-POF11	Information About System	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 system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	5	
CC2.3 POPT 2 Commissions Spanish ACP/A 1 had services Critical (ISC) for specific comits wording. CC2.3 POPT 3 Commissions Spanish ACP/A 1 had services Critical (ISC) for specific comits wording. CC2.3 POPT 3 Commissions Spanish ACP/A 1 had services Critical (ISC) for specific comits wording. CC2.3 POPT 3 Commissions Spanish ACP/A 1 had services Critical (ISC) for specific comits wording. CC2.3 POPT 3 Commissions Spanish College Spanish ACP/A 1 had services Critical (ISC) for specific comits wording. CC2.3 POPT 3 Commissions Spanish College Spanish ACP/A 1 had services Critical (ISC) for specific comits wording. CC2.3 POPT 3 Commissions Spanish College Spanish ACP/A 1 had services Critical (ISC) for specific comits wording. CC2.3 POPT 3 Commissions Spanish College Spanish ACP/A 1 had services Critical (ISC) for specific comits wording. CC2.3 POPT 3 Commissions Spanish College Spanish ACP/A 1 had services Critical (ISC) for specific comits wording. CC2.3 POPT 3 Commissions Spanish College Spanish ACP/A 1 had services Critical (ISC) for specific comits wording. CC2.3 POPT 3 Commissions Spanish College Spanish ACP/A 1 had services Critical (ISC) for specific comits wording. CC2.3 POPT 3 Commissions Spanish College Spanish ACP/A 1 had services Critical (ISC) for specific comits wording. CC2.3 POPT 3 Commissions Spanish College Spanish ACP/A 1 had services Critical (ISC) for specific comits wording. CC2.3 POPT 3 Commissions Spanish College Spanish Spanish College Spanish Spanis	CC2.2-POF12		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		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	
CC2 3 POT 12 Communicate Splane Control (ACPA 5 Trust Services Cheek (TC)) for specific control wording. CC2 3 POT 13 Communicate Splane Commun	CC2.2-POF12		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
CC3 POT3 Communicate System Objectives CC3 POT3 Communicate System Objective S	CC2.2-POF12		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Privacy Awareness	SAT-02	education and training that is relevant for their job function.	5	
CC2 3 POP 13 Communicates Spetial Development ACPA's Trust Services Chiefe (TSC) for specific control wording. CC2 3 POP 14 Communicates Spetial Development ACPA's Trust Services Chiefe (TSC) for specific control wording. CC2 3 POP 15 Communicates Spetial Development ACPA's Trust Services Chiefe (TSC) for specific control wording. CC2 3 POP 16 Communicates Spetial Development ACPA's Trust Services Chiefe (TSC) for specific control wording. CC2 3 POP 17 Communicates Spetial Development ACPA's Trust Services Chiefe (TSC) for specific control wording. CC2 3 POP 18 Communicates Spetial Development ACPA's Trust Services Chiefe (TSC) for specific control wording. CC2 3 POP 19 Communicates Spetial Development ACPA's Trust Services Chiefe (TSC) for specific control wording. CC2 3 POP 19 Communicates Spetial Development ACPA's Trust Services Chiefe (TSC) for specific control wording. CC2 3 POP 19 Communicates Spetial Development ACPA's Trust Services Chiefe (TSC) for specific control wording. CC2 3 POP 19 Communicates Spetial Development ACPA's Trust Services Chiefe (TSC) for specific control wording. CC2 3 POP 19 Communicates Spetial Development ACPA's Trust Services Chiefe (TSC) for specific control wording. CC2 3 POP 19 Communicates Spetial Development ACPA's Trust Services Chiefe (TSC) for specific control wording. CC2 3 POP 19 Communicates Spetial Development ACPA's Trust Services Chiefe (TSC) for specific control wording. CC2 3 POP 19 Communicates Spetial Development ACPA's Trust Services Chiefe (TSC) for specific control wording. CC2 3 POP 19 Communicates Spetial Development ACPA's Trust Services Chiefe (TSC) for specific control wording. Functional Interacts with Development Deve	CC2.2-POF12		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		SAT-03	training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and	5	
CC2.2-PCP13 Communicates System Developed ACPNA Trust Enviseo Criteria (TSC) for specific central wording. Functional Intersects with Functional Inters	CC2.2-POF13		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CHG-01	Mechanisms exist to facilitate the implementation of a change management	5	
CC2.2 POPT 3 Communicates System Changes CC2.2 POPT 3 Communicates System CC2.2 POPT 3 Com	CC2.2-POF13	Communicates System	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Change	CHG-02		5	
CC23-POF13 Communicates System Changes CC23-POF13 Communicates System Changes CCC3-POF13 Communicates System Changes Communicates System Communica	CC2.2-POF13	Communicates System	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Stakeholder Notification	CHG-05		5	
CC22-PDF13 Connunciates System Changes Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Connunciations System State Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Project Control wording. Functional intersects with Control with Air Pro	CC2.2-POF13	Communicates System	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Role-Based Cybersecurity	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and	5	
CC2.3 COSO Principle 15 Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC2.3 COSO Principle 15 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Contacts With District Services Criteria (TSC) for specific control wording. Functional intersects with Contacts With District Services Criteria (TSC) for specific control wording. CC2.3 COSO Principle 15 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Contacts With Authorities Contacts With District Services Criteria (TSC) for specific control wording. Functional intersects with Contacts With Groups & Associations CC2.3 COSO Principle 15 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Contacts With Co	CC2.2-POF13		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Communications & Anomalous System	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators	5	
CC2.3 COSO Principle 15 Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC2.3 COSO Principle 15 Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC2.3 COSO Principle 15 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with control wording. Functional intersects with Corust With Authorities (GOV-GOV-GOV-GOV-GOV-GOV-GOV-GOV-GOV-GOV-	CC2.3	COSO Principle 15	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Statutory, Regulatory &	CPL-01		5	
CC2.3 COSO Principle 15 Download AiCPA's Trust Services Criteria (TSC) for specific control wording. CC2.3 COSO Principle 15 Download AiCPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Contacts with Contacts with Contact with selected groups and associations within the operaceurity & data privacy communities to: (1) Facilitate and congoing operaceurity & data privacy communities to: (1) Facilitate and congoing operaceurity & data privacy practices, techniques and techniques and techniques and incidents. (2) Mariantal currency with recommended operaceurity & data privacy practices, techniques and techniques and incidents. (3) Share current operaceurity and/or data privacy-related information including threats understabilities and incidents. (3) Share current operaceurity and/or data privacy-related information including threats understabilities and incidents. (3) Share current operaceurity and/or data privacy-related information including threats understabilities and incidents. (3) Share current operaceurity and/or data privacy-related information including threats understabilities and incidents. (3) Share current operaceurity and/or data privacy-related information including threats understabilities and incidents. (4) Incident Stakeholders; (4) Affected cleans & Britic-parties; and (3) Alexandra and incidents; (4) Affected cleans & Britic-parties; and (3) Alexandra understabilities and long and according to the privacy practices, techniques and techniques and information including threats understabilities and incidents and incidents. (4) Incident Stakeholders; (4) Affected cleans & Britic-parties; and (3) Alexandra understabilities and long and according to the privacy practices, techniques and techniques and incidents. (5) Affected cleans & Britic-parties; and (3) Alexandra understabilities and contract with applicable and long and according to the privacy practices, techniques and information incidents. (6) Alexandra parties and techniques and contract	CC2.3	COSO Principle 15	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Controls	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
CC2.3 COSO Principle 15 Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC2.3 COSO Principle 15 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Interse	CC2.3	COSO Principle 15	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		GOV-06	enforcement and regulatory bodies.	5	
CC2.3 COSO Principle 15 Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC2.3 COSO Principle 15 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Regulatory A Law Enforcement Contacts. IBC-14 Enforcement Contact with applicable regulatory and law enforcement Regions and law enforcement Regions with applicable regulatory and law enforcement Regions. CC2.3 COSO Principle 15 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Processing Activities Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Processing Activities Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Processing Activities Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Registration Regi	CC2.3	COSO Principle 15	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		GOV-07	the cybersecurity & data privacy communities to: (1) Facilitate ongoing cybersecurity & data privacy education and training for organizational personnel; (2) Maintain currency with recommended cybersecurity & data privacy practices, techniques and technologies; and (3) Share current cybersecurity and/or data privacy-related information including	5	
CC2.3 COSO Principle 15 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Principle PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities PRI-14 Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities	CC2.3	COSO Principle 15	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;	5	
CC2.3 COSO Principle 15 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Processing Activities CC2.3-POF1 Communicates to External Parties CC2.3-POF5 Communicates to Communicate to Communica						Regulatory & Law		(3) Regulatory authorities. Mechanisms exist to maintain incident response contacts with applicable regulatory		
CC2.3 COSO Principle 15 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with processing Activities pro								Mechanisms exist to document Personal Data (PD) processing activities that cover		
External Parties Reporting (2) Affected clients & Intri-parties; and (3) Regulatory submittees. Communicates to		Communicates to				Processing Activities Incident Stakeholder		disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements. Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders;		
								(3) Regulatory authorities.		
CP2 3.DRS Communicates to Described AICRA's Trust Sendoral Children's		External Parties Communicates to				for Sensitive Data Supply Chain				
External Parties Coordination Chain for systems or system components related to the incident. Coordination With Coordinatio		Enables Inbound				Coordination With		chain for systems or system components related to the incident. Mechanisms exist to establish a direct, cooperative relationship between the		
Communications Externs Providers Mechanisms exist to define supporting business processes and implement Service Delivery appropriate governance and service management to ensure appropriate planning,						Service Delivery		Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning,		
CUZ-3-PUP2 Communications Communications Download AICPA's frust services Criteria (ISC) for specific control wording. Functional intersects with intersects wi		Communications				Support)		business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area. Mechanisms exist to require contractual requirements for cybersecurity & data		
CC2.3-POF2 Communications Com	CC2.3-POF2	Communications	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Requirements	TPM-05	its systems, processes and data.	5	
CC2.3-POF3 Communicates With the Board of Directors Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Intersects with Pownload AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Intersects with Program Oversight Program Oversight Program Oversight Mechanisms exist to provide governance oversight reporting and recommendations	CC2.3-POF3	Board of Directors	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	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	
CC2.3-POFS 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 Directors Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Governing Body Directors Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Governing Body Directors Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Governing Body Michanism sexist to facilitate the implementation of personnel security controls.		Board of Directors	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Governing Body	GOV-01.2	to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
CC2.3-POF4 Communication Lines Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Security Management HRS-01 5	CC2.3-POF4	Communication Lines	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		HRS-01		5	
Provides Separate Communication Lines Provides Separate Communication Lines Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Workplace Investigations HRS-07.1 reasonable assurance that a policy has been violated. 5	CC2.3-POF4		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		HRS-07.1	reasonable assurance that a policy has been violated.	5	
CC2.3-POF5 Selects Relevant Method Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Protection Government Color Governmen										



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)
CC2.3-POF5	Selects Relevant Method of Communication	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 & data protection program.	5	
CC2.3-POF5	Selects Relevant Method of Communication	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	
CC2.3-POF6	Communicates Objectives Related to Confidentiality and Changes to Those Objectives	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	
CC2.3-POF6	Communicates Objectives Related to Confidentiality and Changes to Those	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	standards to achieve the specific goals of the process area. Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
CC2.3-POF6	Ohiectives Communicates Objectives Related to Confidentiality and Changes to Those Objectives	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 & data privacy controls between internal stakeholders and External Service Providers (ESP).	5	
CC2.3-POF7	Communicates Objectives 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	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.	5	
CC2.3-POF7	Objectives Communicates Objectives Related to Privacy and Changes to Those Objectives	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 as 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 orterial required by applicable statutory, regulatory and contractuated orterial required by applicable statutory, regulatory and contractuated orterial required by applicable statutory, regulatory and contractuation of the processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice. (3) Personationally, review and update the content of the privacy notice, as necessary; and the privacy notice, in accordance with data retention requirements.	5	
CC2.3-POF7	Communicates Objectives Related to Privacy and Changes to Those Objectives	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 & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
CC2.3-POF8	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; (6) Eradication; and	5	
CC2.3-POF8	Communicates Incident Reporting Methods	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 document, monitor and report the status of cybersecurity &	5	
CC2.3-POF8	Communicates Incident Reporting Methods	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Situational Awareness For Incidents	IRO-09	data privacy incidents to internal stakeholders all the way through the resolution of the incident.	5	
CC2.3-POF8	Communicates Incident Reporting Methods	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-POF9	Operation and Boundaries	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	10	
CC2.3-POF9	Communicates Information About System Operation and Boundaries	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	
CC2.3-POF9	Communicates Information About System Operation and Boundaries	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (PASCI) matrix, or similar documentation, to delineate assignment for ophersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs). Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar	10	
CC2.3-POF10	Communicates System Objectives	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	System Security & Privacy Plan (SSPP)	IAO-03	document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	5	
CC2.3-POF10	Communicates System Objectives	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique	5	
CC2.3-POF10	Communicates System Objectives	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Management	TPM-01	business needs. Mechanisms exist to facilitate the implementation of third-party management controls.	5	
CC2.3-POF10	Communicates System Objectives	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 & data privacy requirements with third-parties, reflecting the organization's needs to protect	5	
CC2.3-POF11	Communicates System Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	System Security & Privacy Plan (SSPP)	IAO-03	Its systems, processes and data. Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications earlier, positions or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its	5	
CC2.3-POF11	Communicates System Responsibilities	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 & data privacy requirements with third-parties, reflecting the organization's needs to protect	5	
CC2.3-POF11	Communicates System Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Responsible, Accountable, Supportive, Consulted & Informed	TPM-05.4	Its systems, crocesses and data. Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal	10	
CC2.3-POF12	Communicates Information on Reporting	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(RASCI) Matrix Cyber Incident Reporting for Sensitive Data	IRO-10.2	stakeholders and External Service Providers (ESPs). Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
CC2.3-POF12	Sustem Failures Communicates Information on Reporting	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Coordination With	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	5	
CC2.3-POF12	System Failures. Communicates Information on Reporting System Failures, Incidents, Concerns, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Suspicious Communications & Anomalous System	SAT-03.2	Mechanisms exist to provide training to personned on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
CC2.3-POF12	Other Matters Communicates Information on Reporting	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Behavior Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
GGZ.SFUFIZ	System Failures, Communicates	2700 A 7 TOUR CONTROL OF THE 12 OF THE SPECIAL CONTROL WORKING.	, anotionat	muraeus With	ary management		Mechanisms exist to require contractual requirements for cybersecurity & data	,	
CC2.3-POF12	Information on Reporting System Failures, Incidents, Concerns, and Other Matters Communicates	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data. Mechanisms exist to compel External Service Providers (ESPs) to provide notification	5	
CC2.3-POF12	Information on Reporting System Failures, Incidents, Concerns, and Other Matters	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security Compromise Notification Agreements	TPM-05.1	of actual or potential compromises in the supply chain that can potentially affect or have adversely affected systems, applications and/or services that the organization utilizes.	5	
CC2.3-POF12	Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters	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 & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
CC3.1	COSO Principle 6	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	10	
CC3.1	COSO Principle 6	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Privacy Portfolio	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy- related resource planning controls that define a viable plan for achieving	5	
CC3.1	COSO Principle 6	Download AICPA's Trust Services Criteris (TSC) for specific control wording.	Functional	intersects with	Management Cybersecurity & Data Privacy In Project Management	PRM-04	cybersecurity & data prixacy objectives. Mechanisms exist to assess cybersecurity & data prixacy 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 exactle at the control control of the c	5	
	+	<u> </u>	1	l	1		meeting the requirements.	-	



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 define business processes with consideration for cybersecurity & data privacy that determines:	(optional)	
CC3.1	COSO Principle 6	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	COSO Principle 6	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 develop a plan for Supply Chain Risk Management (SCRM)	5	
CC3.1	COSO Principle 6	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	associated with the development, acquisition, maintenance and disposal of	5	
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 & data privacy principles that addresses risk to organizational operations, assets, individuals, other	5	
CC3.1-POF1	Reflects Management's Choices	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Define Control Objectives	GOV-09	organizations. Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5	
CC3.1-POF1	Reflects Management's Choices	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-POF1	Reflects Management's Choices	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;	5	
CC3.1-POF1	Reflects Management's	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	5	
CC3.1-POF1	Choices Reflects Management's	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Threshold	RSK-01.4	acceptable results. 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	Choices Reflects Management's	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	5	
CC3.1-POF2	Choices Considers Tolerances for Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Risk Tolerance	RSK-01.3	organization is willing to accept in anticipation of a reward. 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	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	Machanisms axist to define the context of its husiness model and document the	5	
CC3.1-POF3	Includes Operations and Financial Performance Goals	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Framing	RSK-01.1	reclaims due to descript in Assessments (ask response and risk monitoring: (1) Assumptions affecting risk assessments, risk response and risk monitoring: (3) The against amount of the assessment of the assessment of the monitoring (3) The against amount of the description of the assessment of the as	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	Cybersecurity & Data Privacy Portfolio Management	PRM-01		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		5	
CC3.1-POF5	Complies With Applicable	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Operationalizing Cybersecurity & Data	GOV-15	projects / initiatives. Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service	5	
CC3.1-POF5	Accounting Standards Complies With Applicable	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection Practices Statutory, Regulatory &	CPL-01	under their control. Mechanisms exist to facilitate the identification and implementation of relevant	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	statutory, regulatory and contractual controls. Mechanisms exist to define materiality threshold criteria capable of designating an	5	
CC3.14F0F6	Considers Materiality	DOWNROAD AICEA S IT DE SERVICES CITERIA (15C) FOI SPECIAL COMMON WORKING.	Functional	intersects with	Plateriality Determination	304-10	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 (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
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. Mechanisms exist to define supporting business processes and implement	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 Support)	OPS-03	appropriate governance and service management to ensure appropriate planning,	5	
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	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy the determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and organizations; and organizations; and of the organizations; and organizations; and organizations; and organizations; and organizations; and organizations; and organizations organizations; and organizations organizations organizations or created and organizations or created and organizations or considerations or cons	5	
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	
CC3.1-POF8	Compties With Externally Established Frameworks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
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	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy the 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 chitation.)	5	
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,	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	
CC3.1-POF9	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	business functions, workforce, and/or customers based on industry-recognized	5	
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	(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-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.:	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
CC3.1-POF10	Reflects Entity Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies. Mechanisms exist to submit satus reporting of the organization's cybersecurity	5	
CC3.1-POF10	Reflects Entity Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Privacy Status Reporting	GOV-17	and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	5	
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 organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific peals of the process area.	5	



cure 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	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and cybersecond organizations of cybersecond 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	
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	obtained Mechanism 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	
CC3.1-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	regular basis. Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
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 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 societic goods of the orccess sure.	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	Mechanisms exist to define business processes with consideration for cybersecurity & date privacy that determines: (1) The resulting risk to or ganizational operations, assets, individuals and other organizations; and (2) information processes and cybersecurity of the companies of the cybersecurity of the cybersecurity of the cybersecurity of the cybersecurity of the cybersecurity of the cybersecurity of the cybersecurity of the cybersecurity of the cybersecurity of the cybersecurity of the cybersecurity of the cybersecurity of the cybersecurity of the cybersecurity of the cybersecurity of the cybers	5	
CC3.1-POF12	Considers the Required Level of Precision	Download AIGPA'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 solview the suceptic cools 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 & data privacy the 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-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	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate ghaning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards for anothers the service model of the noncess area.	5	
CC3.1-POF13	Reflects Entity 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 & data privacy 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	
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 solview the seceptic costs 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 & data privacy that determines: (1) The resulting risk to or ganizational 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 nixtuned.	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, detelvery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized actionarists to arbitrate the societies and of the noroneas were activated and the societies and of the noroneas were supported and the societies and of the noroneas were supported and the societies and of the noroneas were supported and the societies and the noroneas were supported as the societies and the noroneas were supported as the normal supported as the noroneas were supported as the noroneas were supported as the normal supported as the noroneas were supported as the noroneas and the noroneas are supported as the noroneas are suppo	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	Mechanisms exist to define business processes with consideration for cybersecurity & date privacy that determines: (1) The resulting risk to or garizational operations, assets, individuals and other organizations; and cybersecond organizations of cybersecond organizations; and (2) Information protection needs arising from the defined business processes and revises the processes an encessary, until an achievable set of protection needs is	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	chtrainer! 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 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 sociefic cools of the process area.	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	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy 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 advantaged.	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 Section; 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 fisk.	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, disrutotion, modification or destruction of the organization's systems and data. Mechanisms exist to identify:	5	
CC3.2	Considers Tolerances for Risk	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 relating 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	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 systems and data in accordance with applicable laws, regulations and contractual collegations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5	
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 Considers Tolerances for Risk	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	Business Impact Analysis (BIA) Supply Chain Risk Management (SCRM) Plan	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BlA) to identify and assess coherescentify and data protection fisks. Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) sascolated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected spitalisation actions and maintenance proferonace assessing those along contributions and maintenance proferonace assessing those along spitalisation actions and maintenance and proferonace assessing those along spitalisation actions and maintenance and proferonace assessing the action spitalisation actions and maintenance and proferonace assessing those along spitalisation actions and maintenance and spitalisation actions spitalisation actions and spitalisation actions spitalisation actions spitalisation acti	5	
	Considers Tolerances for				Data Protection Impact		mitigating actions and monitoring performance against those plans. Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on		
CC3.2	Risk	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Assessment (DPIA)	RSK-10	systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
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 & data privacy practices in the specification, design, development,	5	
	Includes Entity,				Risk Management		implementation and modification of systems and services. Mechanisms exist to facilitate the implementation of strategic, operational and		
CC3.2-POF1	Subsidiary, Division, Operating Unit, and Includes Entity,	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Program	RSK-01	tactical risk management controls. Mechanisms exist to identify and document risks, both internal and external.	10	
CC3.2-POF1	Subsidiary, Division, Operating Unit, and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Identification	RSK-03		5	
CC3.2-POF1	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 systems and data. Mechanisms exist to identify:	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	(1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The originational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
CC3.2-POF2	Analyzes Internal and	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	External Factors Analyzes Internal and	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,	5	
CC3.2-P0F3	External Factors Involves Appropriate	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data	GOV-17	disruption. modification or destruction of the organization's systems and data. Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as	5	
CC3.2-POF3	Levels of Management Involves Appropriate	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Privacy Status Reporting Risk Management	RSK-01	required. Mechanisms exist to facilitate the implementation of strategic, operational and	10	
CC3.2-POF3	Levels of Management Involves Appropriate	Download AICPA's Trust Services Criteria (TSC) for specific control wording.			Program	RSK-04	tactical risk management controls. Mechanisms exist to conduct recurring assessments of risk that includes the		
	Levels of Management Estimates Significance of	· · · · · · · · · · · · · · · · · · ·	Functional	equal	Risk Assessment		likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data. Mechanisms exist to prioritize the impact level for systems, applications and/or	10	
CC3.2-POF4	Risks Identified Estimates Significance of	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	Impact-Level Prioritization Risk Ranking	RSK-02.1	services to prevent potential disruptions. Mechanisms exist to identify and assign a risk ranking to newly discovered security	5	
CC3.2-POF4	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	subset of	Risk Management	RSK-01	vulnerabilities that is based on industry-recognized practices. Mechanisms exist to facilitate the implementation of strategic, operational and	10	
CC3.2-POF5	Respond to Risks Determines How to		Functional	equal	Program Risk Response	RSK-06.1	tactical risk management controls. Mechanisms exist to respond to findings from cybersecurity & data privacy sessessment; inclidents and suittle to ensure proper remediation has been	10	
	Respond to Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.		,		RSK-06.1	assessments, incidents and audits to ensure proper remediation has been <u>performed</u> . Mechanisms exist to identify and document risks, both internal and external.		
CC3.2-POF6	Identifies Threats	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Identification		Mechanisms exist to develop and keep current a catalog of applicable risks	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	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 systems and data.	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	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	THR-02	threat hunting, response and recovery activities. Mechanisms exist to develop Indicators of Exposure (IOE) to understand the	5	
CC3.2-POF6	Identifies Threats	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(IOE) Threat Intelligence Feeds	THR-03	potential attack vectors that attackers could use to attack the organization. Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures	5	
					Feeds		to facilitate the implementation of preventative and compensating controls. Mechanisms exist to develop and keep current a catalog of applicable internal and		
CC3.2-POF6	Identifies Threats	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	Threat Catalog Threat Analysis	THR-09	external threats to the organization, both natural and manmade. Mechanisms exist to identify, assess, prioritize and document the potential impact(s	5	
	Identifies Vulnerability of				Supply Chain Risk		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		
CC3.2-POF7	System Components	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management (SCRM) Plan	RSK-09	systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	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 Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	5	
CC3.2-POF7	Identifies Vulnerability of System Components	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, response and recovery activities.	5	
CC3.2-POF7	Identifies Vulnerability of System Components	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	
CC3.2-POF7	Identifies Vulnerability of System Components	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. Mechanisms exist to:	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	rectnismisms exists: (I) Evaluate security risks and threats associated with the services and product supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	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	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
CC3.2-POF7	Identifies Vulnerability of System Components	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	
CC3.2-POF7	Identifies Vulnerability of System Components	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Vulnerability Scanning	VPM-06	management activities. Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	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	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) Pinoties, benefits and trade-offs considered by the organization for managing risk.	5	
CC3.2-POF8	Analyzes Threats and Vulnerabilities From Vendors, Business	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	Partners and Other Analyzes Threats and Vulnerabilities From Vendors, Business	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	Partners, and Other Analyzes Threats and Vulnerabilities From Vendors, Business	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	Partners, and Other Analyzes Threats and Vulnerabilities From Vendors, Business	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 systems and data.	5	
CC3.2-POF8	Partners, and Other Parties Analyzes Threats and Vulnerabilities From Vendors, Business	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	Partners, and Other 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 systems, system components and services, including documenting selected	5	
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 Criticality Assessments	TPM-02	mitigating actions and monitoring performance against those plans. Mechanisms exist to identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
CC3.2-POF8	Parties Analyzes Threats and Vulnerabilities From Vendors, Business	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 services.	5	
CC3.2-POF8	Partners and Other Analyzes Threats and Vulnerabilities From Vendors, Business	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6		5	
	Partners, and Other Parties						controls, including any flow-down requirements to subcontractors.		



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)
							Mechanisms exist to conduct recurring assessments of risk that includes the	(optional)	
							likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.		
CC3.2-POF9	Assesses the Significance of the Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Assessment	RSK-04		5	
							Mechanisms exist to periodically assess supply chain risks associated with systems,		
							system components and services.		
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		5	
							Mechanisms exist to identify, prioritize and assess suppliers and partners of critical		
							systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.		
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	retailed to their importance in supporting the delivery of ingrivative services.	5	
	Of the Risks				Assessments				
							Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.		
CC3.2-POF9	Assesses the Significance	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Risk	TPM-04.1		5	
	of the Risks				Assessments & Approvals				
							Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.		
CC3.2-POF9	Assesses the Significance	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Threat Analysis	THR-10		5	
CC3.2-FOF8	of the Risks	Downtoad AICEA'S Trust Services Citeria (13C) for specific control wording.	Functional	ilitersects with	IIII eat Allatysis	IIIN-10		3	
							Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.		
	Assesses the Significance			later 1	Vulnerability & Patch	we		_	
CC3.2-POF9	of the Risks	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management Program (VPMP)	VPM-01		5	
							Mechanisms exist to define and manage the scope for its attack surface		
	A						management activities.		
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		5	
							Mechanisms exist to identify, assess, prioritize and document the potential impact(s)		
							and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.		
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		5	
					-				
							Mechanisms exist to implement a threat intelligence program that includes a cross-		
CC3.3	COSO Principle 8	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	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,	10	
					-		threat hunting, response and recovery activities.		
CC3.3	COSO Principle 8	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	
CC3.3	COSO Principle 8	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross- discipline insider threat incident handling team.	5	
CC3.3	COSO Principle 8	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	
CC3.3	COSO Principle 8	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique systems, system components or	5	
CC3.3	COSO Principle 8	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Services	TPM-04	services. Mechanisms exist to mitigate the risks associated with third-party access to the	5	
							organization's systems and data. Mechanisms exist to ensure that the interests of external service providers are		
CC3.3	COSO Principle 8 Considers Various Types	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Conflict of Interests	TPM-04.3	consistent with and reflect organizational interests. Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement	5	
CC3.3-POF1	of Fraud Considers Various Types	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Asset Governance Human Resources	AST-01	and manage asset management controls. Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC3.3-POF1	of Fraud	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security Management	HRS-01	Mechanisms exist to implement a threat intelligence program that includes a cross-	5	
CC3.3-POF1	Considers Various Types	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Threat Intelligence Feeds	THR-01	organization information-sharing capability that can influence the development of	10	
	of Fraud				Program		the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.		
CC3.3-POF1	Considers Various Types of Fraud	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross- discipline insider threat incident handling team.	5	
CC3.3-POF2	Assesses Incentives and Pressures	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	
	Assesses Incentives and	D	I		Threat Intelligence Feeds	T1:-	Mechanisms exist to implement a threat intelligence program that includes a cross- organization information-sharing capability that can influence the development of		
CC3.3-POF2	Pressures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Program	THR-01	organization information-sharing capability that can intuence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
CC3.3-POF2	Assesses Incentives and	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-	10	
CC3.3-POF3	Pressures Assesses Opportunities	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	
					Security Management	-	Mechanisms exist to implement a threat intelligence program that includes a cross-		
CC3.3-POF3	Assesses Opportunities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	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,	10	
							threat hunting, response and recovery activities. Mechanisms exist to implement an insider threat program that includes a cross-		
CC3.3-POF3	Assesses Opportunities Assesses Attitudes and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Insider Threat Program Human Resources	THR-04	discipline insider threat incident handling team. Mechanisms exist to facilitate the implementation of personnel security controls.	10	
CC3.3-POF4	Rationalizations	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security Management	HRS-01	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	5	
CC3.3-POF4	Assesses Attitudes and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	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	
550.51.014	Rationalizations	San Sanona (199) to appeal to control worlding.	. anotoliat	_3000.01	Program		the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.		
CC3.3-POF4					· ·		Mechanisms exist to implement an insider threat program that includes a cross-	10	
	Assesses Attitudes and Rationalizations	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Insider Threat Program	THR-04	I discipline insider threat incident handling team	10	
CC3 3-POF5	Rationalizations Considers the Risks				Human Resources		discipline insider threat incident handling team. Mechanisms exist to facilitate the implementation of personnel security controls.		
CC3.3-POF5	Rationalizations Considers the Risks Related to the Use of IT and Access to Information	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	_	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
CC3.3-POF5	Rationalizations Considers the Risks Related to the Use of IT				Human Resources Security Management Threat Intelligence Feeds		Mechanisms exist to facilitate the implementation of personnel security controls. Mechanisms exist to implement a threat intelligence program that includes a cross- organization information-sharing capability that can influence the development of		
	Rationalizations Considers the Risks Related to the Use of IT and Access to Information 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. 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, reacones and recovery activities.	5	
	Rationalizations Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Human Resources Security Management Threat Intelligence Feeds	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls. Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, montrolling values or security activations.	5	
CC3.3-POF5	Rationalizations Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information Considers the Risks	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 Security Management Threat Intelligence Feeds Program Insider Threat Program Change Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls. Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of intelligence or a control of the control of	5	
CC3.3-POF5 CC3.3-POF5 CC3.4	Rationalizations Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information COSO Principle 9	Download AICPA's Trust Services Criteria (TSC) for specific control worlding. Download AICPA's Trust Services Criteria (TSC) for specific control worlding. Download AICPA's Trust Services Criteria (TSC) for specific control worlding. Download AICPA's Trust Services Criteria (TSC) for specific control worlding.	Functional Functional Functional Functional	intersects with subset of subset of subset of	Human Resources Security Management Threat Intelligence Feeds Program Insider Threat Program Change Management Program Configuration Change	HRS-01 THR-01 THR-04 CHG-01	Mechanisms exist to facilitate the implementation of personnel security controls. Mechanisms exist to implement a threat intelligence program that includes a cross- organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities. Mechanisms exist to implement an insider threat program that includes a cross- discipline insider threat incident handling team.	5 10 10	
CC3.3-POF5	Rationalizations Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information	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 subset of subset of	Human Resources Security Management Threat Intelligence Feeds Program Insider Threat Program Change Management Program Configuration Change Control	HRS-01 THR-01 THR-04	Mechanisms exist to facilitate the implementation of personnel security controls. Mechanisms exist to implement a threat intelligence program that includes a cross- organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat huntins, resoonse and recovery activities. Mechanisms exist to implement an insider threat program that includes a cross- discipline insider threat incident handling team. Mechanisms exist to facilitate the implementation of a change management program. Mechanisms exist to govern the technical configuration change control processes.	10	
CC3.3-POF5 CC3.3-POF5 CC3.4	Rationalizations Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information COSO Principle 9	Download AICPA's Trust Services Criteria (TSC) for specific control worlding. Download AICPA's Trust Services Criteria (TSC) for specific control worlding. Download AICPA's Trust Services Criteria (TSC) for specific control worlding. Download AICPA's Trust Services Criteria (TSC) for specific control worlding.	Functional Functional Functional Functional	intersects with subset of subset of subset of	Human Resources Security Management Threat Intelligence Feeds Program Insider Threat Program Change Management Program Configuration Change	HRS-01 THR-01 THR-04 CHG-01	Mechanisms exist to facilitate the implementation of personnel security controls. Mechanisms exist to implement a threat intelligence program that includes a cross- organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, resonnee and recovery activities. Mechanisms exist to implement an inside threat program that includes a cross- discipline insider threat incident handling team. Mechanisms exist to facilitate the implementation of a change management program. Mechanisms exist to govern the technical configuration change control processes. Mechanisms exist to appropriately test and document proposed changes in a non- production environment before changes are implemented in a production	5 10 10	
CC3.3-POF5 CC3.3-POF5 CC3.4 CC3.4	Rationalizations Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information COSO Principle 9 COSO Principle 9 COSO Principle 9	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	subset of subset of subset of intersects with	Human Resources Security Management Threat Intelligence Feeds Program Insider Threat Program Change Management Program Configuration Change Control Test, Validate & Document Change Cybersecurity & Data	HRS-01 THR-01 THR-04 CHG-01 CHG-02 CHG-02.2	Mechanisms exist to facilitate the implementation of personnel security controls. Mechanisms exist to implement a threat intelligence program that includes a cross- organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat huntine, resonnee and recovery activities. Mechanisms exist to implement an insider threat program that includes a cross- discipline insider threat incident handling team. Mechanisms exist to facilitate the implementation of a change management program. Mechanisms exist to facilitate the implementation of a change ontrol processes. Mechanisms exist to appropriately test and document proposed changes in a non- production environment before changes are implemented in a production environment. Mechanisms exist to include a cybersecurity and/or data privacy representative in	5 10 10 10 5 5	
CC3.3-POF5 CC3.3-POF5 CC3.4 CC3.4	Rationalizations Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Considers the Risks Related to the Use of IT and Access to Information COSO Principle 9 COSO Principle 9	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 subset of subset of subset of intersects with	Human Resources Security Management Threat Intelligence Feeds Program Insider Threat Program Change Management Change Management Contiguration Change Control Test, Validate & Document Changes	HRS-01 THR-01 THR-04 CHG-01 CHG-02	Mechanisms exist to facilitate the implementation of personnel security controls. Mechanisms exist to implement a threat intelligence program that includes a cross- organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat huntine, response and recovery architectures, threat huntine, response and recovery architectures, threat huntine, response and recovery architectures which inside threat includes a cross- discipline inside threat threat includes a cross- discipline inside threat t	5 10 10 10	
CC3.3-POF5 CC3.3-POF5 CC3.4 CC3.4	Rationalizations Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information COSO Principle 9 COSO Principle 9 COSO Principle 9	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	subset of subset of subset of intersects with	Human Resources Security Management Threat Intelligence Feeds Program Insider Threat Program Change Management Program Configuration Change Control Change Control Change Control Change Control Change Control Change Control Change Security Impact Analysis Security Impact Analysis Security Impact Analysis	HRS-01 THR-01 THR-04 CHG-01 CHG-02 CHG-02.2	Mechanisms exist to facilitate the implementation of personnel security controls. Mechanisms exist to implement a threat intelligence program that includes a cross- organization information-sharing capability with acta influence the development of in- trace that instance and recovers activations. Amount of the control	5 10 10 10 5 5	
CC3.3-POF5 CC3.4 CC3.4 CC3.4 CC3.4 CC3.4	Rationalizations Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information COSO Principle 9 COSO Principle 9 COSO Principle 9 COSO Principle 9	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	subset of subset of subset of intersects with intersects with intersects with	Human Resources Security Management Threat Intelligence Feeds Program Insider Threat Program Change Management Program Configuration Change Control Test, Validate & Document Changes Control Test, Validate & Document Changes Security Ingock Changes Security Ingock Changes Security Ingock Changes For Changes Control Ch	HRS-01 THR-01 THR-04 CHG-01 CHG-02 CHG-02.2 CHG-02.3 CHG-03	Mechanisms exist to facilitate the implementation of personnel security controls. Mechanisms exist to implement a threat intelligence program that includes a cross- organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring. Mechanisms exist to implement an insider threat program that includes a cross- discipline insider threat incident handling team. Mechanisms exist to implement an insider threat program that includes a cross- discipline insider threat incident handling team. Mechanisms exist to give the technical configuration change control processes. Mechanisms exist to give me the technical configuration change control processes. Mechanisms exist to appropriately test and document proposed changes in a non- production environment before changes are implemented in a production environment. Mechanism exist to includes a ophereculty and/or data privacy representative in the configuration change control review process. Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5 10 10 10 5 5 5 5 5	
CC3.3-POF5 CC3.3-POF5 CC3.4 CC3.4 CC3.4	Rationalizations Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information Considers the Risks Related to the Use of IT and Access to Information COSO Principle 9 COSO Principle 9 COSO Principle 9	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	subset of subset of subset of intersects with intersects with	Human Resources Security Management Threat Intelligence Feeds Program Insider Threat Program Change Management Pootena Configuration Change Control Test, Validate & Document Change Cybersecurity & Data Privacy Representative for Asset Lifecylec Dataset Lifecylect Mayer Security (Impact Analysis for Changes)	HRS-01 THR-01 THR-04 CHG-01 CHG-02 CHG-02.2	Mechanisms exist to facilitate the implementation of personnel security controls. Mechanisms exist to implement a threat intelligence program that includes a cross- organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring threat hunting, response and recovery activities. Mechanisms exist to implement an inside threat program that includes a cross- discipline insider threat incident handling team. Mechanisms exist to facilitate the implementation of a change management program. Mechanisms exist to govern the technical configuration change control processes. Mechanisms exist to propositistly test and document proposed changes in a non- production environment before changes are implemented in a production mechanisms exist to include a cybersecurity and/ord data privacy representative in the configuration change control review process.	5 10 10 10 5 5 5 5	



Secure 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 (optional)	Notes (optional)
							Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines:	,-,-,-,-,	
CC3.4	COSO Principle 9	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		
CC3.4	COSO Principle 9	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Risk	TPM-04.1	obtained Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
000.4	occor mape o	Somious Act As Trad out the something (100) to specific contact trouing.	Tunctional	mulacus with	Assessments & Approvals		Mechanisms exist to monitor, regularly review and assess External Service Providers		
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 & data privacy 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 information, systems and processes that are in scope by	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 Management Program	RSK-01	the third-party. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
CC3.4-POF1	Assesses Changes in the External Environment	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-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	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	Assesses Changes in the	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Management	RSK-01	disruption. modification or destruction of the organization's systems and data. Mechanisms exist to facilitate the implementation of strategic, operational and	5	
CC3.4-POF2	Business Model	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Program	HSK-UI	tactical risk management controls. Mechanisms exist to identify and document risks, both internal and external.	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		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 Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure,	5	
	Assesses Changes in				Steering Committee &		disruption, modification or destruction of the organization's systems and data. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key		
CC3.4-POF3	Leadership	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Program Oversight	GOV-01.1	cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
CC3.4-POF3	Assesses Changes in Leadership	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.	5	
CC3.4-POF3	Assesses Changes in Leadership	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-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 systems and data.	5	
CC3.4-POF4	Assesses Changes in Systems and Technology	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change Management Program	CHG-01	disruption, modification or destruction of the organization's systems and data. Mechanisms exist to facilitate the implementation of a change management program.	5	
CC3.4-POF4	Assesses Changes in Systems and Technology	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	
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.	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-POF4	Systems and Technology	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and occurrent risks, both internal and external. Mechanisms exist to conduct recurring assessments of risk that includes the	5	
CC3.4-POF4	Assesses Changes in Systems and Technology	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 sccess, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
CC3.4-POF5	Assesses Changes in Vendor and Business	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	
CC3.4-POF5	Assesses Changes in Vendor and Business	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-POF5	Assesses Changes in Vendor and Business Partner Relationships	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 systems and data.	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						Mechanisms exist to perform recurring validation of the Responsible, Accountable,		
CC3.4-POF5	Assesses Changes in Vendor and Business	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 & data privacy control assignments accurately reflect current	5	
	Partner Relationships Assesses Changes in						business practices, compliance obligations, technologies and stakeholders. Mechanisms exist to monitor, regularly review and assess External Service Providers		
CC3.4-POF5	Vendor and Business Partner Relationships	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 & data privacy controls.	5	
CC3.4-POF5	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	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business information, systems and processes that are in scope by	5	
	Partner Relationships Assesses Changes in				-		the third-party. Mechanisms exist to implement a threst 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	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	
	Vulnerabilities Assesses Changes in				Vulnerability & Patch		Mechanisms exist to facilitate the implementation and monitoring of vulnerability		
CC3.4-POF6	Threats and Vulnerabilities Assesses Changes in	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management Program (VPMP)	VPM-01	management controls. Mechanisms exist to define and manage the scope for its attack surface	5	
CC3.4-POF6	Threats and Vulnerabilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Attack Surface Scope	VPM-01.1	management activities.	5	
CC3.4-POF6	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	
000 4 000	Vulnerabilities Assesses Changes in	Doubled AICRA's Trust Senier - City - CTC's	E	inter	Vulnerability Exploitation	VPM-03.1	Mechanisms exist to identify, assess, prioritize and document the potential impact(s)	5	
CC3.4-POF6	Threats and Vulnerabilities Assesses Changes in	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Analysis	vrM-03.1	and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities. Mechanisms exist to detect vulnerabilities and configuration errors by routine	ь	
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.	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	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity & data protection policies,	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	CPL-03.2	standards and other applicable requirements. Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	
					Protection Controls		organization's cybersecurity & data protection policies and standards. Mechanisms exist to thoughtfully plan audits by including input from operational risk		
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Audit Activities	CPL-04	and compliance partners to minimize the impact of audit-related activities on business operations.	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	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	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 of the cybersecurity & data privacy program.	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 & Data privacy program. Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Information Assurance	IAO-01	cvbersecurity & data privacy program. Mechanisms exist to facilitate the implementation of cybersecurity & data privacy	5	
554.1		откольторто вреши сописк могату.	. anotoliat	with	(IA) Operations		assessment and authorization controls. Mechanisms exist to formally assess the cybersecurity & data privacy controls in	-	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Assessments	IAO-02	systems, applications and services through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating a intended and producing the desired outcome with personal to meeting	5	
							operating as intended and producing the desired outcome with respect to meeting expected requirements. Mechanisms exist to ensure assessors or assessment teams have the appropriate		
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Assessor Independence	IAO-02.1	independence to conduct cybersecurity & data privacy control assessments.	5	
							Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations;		
							(2) Monitoring capabilities; (3) Mobile devices;		
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Specialized Assessments	IAO-02.2	(4) Databases; (5) Application security; (6) Embedded technologics (a.g., lot, OT, etc.);	5	
							(6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code;		
							(8) Maticious code; (9) Insider threats; (10) Performance/load testing; and/or		
	1				1	l	(14) Artificial Intelligence and Automonous Technologies (AAT)		



Secure Controls Framework (SCF) 15 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)
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Plan / Coordinate with Other Organizational Entities	IAO-03.1	Mechanisms exist to plan and coordinate Information Assurance Program (IAP) activities with affected stakeholders before conducting such activities in order to reduce the potential impact on operations.	5	
CC4.1	COSO Principle 16	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	5	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical cybersecurity & data privacy controls.	5	
CC4.1	COSO Principle 16	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	
CC4.1	COSO Principle 16	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Privacy In Project Management	PRM-04	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 Privacy Requirements Definition	PRM-05	meeting the requirements. Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
CC4.1	COSO Principle 16	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 & data privacy 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 whether or the processes as necessary, until an achievable 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	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM)	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	associated with the development, acquisition, maintenance and disposal of	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 & data privacy principles that addresses risk to organizational operations, assets, individuals, 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	the organization's technology and information governance processes.	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	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/inlegators consult with cybersecurity & data privacy personnal 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	program measures of performance. Mechanisms exist to implement an internal audit function that is capable of	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.	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.	Mechanisms exist to implement an internal sudit 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 sudit 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.	providing conject against the management with incidete into the appropriateness of	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	(1) Statutory, regulatory and contractual comptiance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases;	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.	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.	Mechanisms exist to implement an internal audit function that is capable of	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.	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.	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 & data privacy assessment and authorization controls.	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	Assessments	IAO-02	operating as intended and producing the desired outcome with respect to meeting	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.	expected requirements. 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.	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
CC4.2	COSO Principle 17	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Non-Compliance Oversight	CPL-01.	mitigation actions.	5	
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	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 eliminate known vulnerabilities.	5	
CC4.2	COSO Principle 17	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	
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	process, to objectively identify and remediate vulnerabilities prior to release to production.	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	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements. Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and	5	
CC4.2	COSO Principle 17	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Vulnerability Remediation Process Continuous Vulnerability	VPM-02	remediated.	5	
CC4.2	COSO Principle 17	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	



ecure Controls Framework (SCF) 16 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)
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	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	
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	regular basis. Methods are sixt to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
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 & data privacy program measures of performance.	5	
CC4.2-POF1	Assesses Results	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-POF1	Assesses Results	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 & data protection controls oversight function that reports to the organization's executive leadership.	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	Mechanisms exist to compet data and/or process owners to assess if required cybersecurity & data privacy 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 & 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 & 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 & 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 attiminate known witnershilling.	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	eltiminate known vulnerabilities. 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 & data privacy 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 & data privacy 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	Mechanisms exist to compel data and/or process owners to implement required cybersecurity & data privacy 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	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	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	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	
CC5.1	COSO Principle 10	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security Concept Of Operations (CONOPS)	OPS-02	Mechanisme 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	
CC5.1	COSO Principle 10	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition		Mechanisms exist to define business processes with consideration for cybersecurity & data privacy 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	
CC5.1	COSO Principle 10	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 facilitate the implementation of industry-recognized	5	
CC5.1	COSO Principle 10	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Engineering Principles	SEA-01	reclaims to exist or activate the implementation or industry ecopiese crybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services. Mechanisms exist to centrally-manage the organization-wide management and	5	
CC5.1	COSO Principle 10	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Centralized Management of Cybersecurity & Data Privacy Controls	SEA-01.1	implementation of cybersecurity & data privacy controls and related processes. Mechanisms exist to develop an enterprise architecture, aligned with industry-	5	
CC5.1	COSO Principle 10	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Alignment With Enterprise Architecture Operationalizing	SEA-02	recognized leading practices, with consideration for ophersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations. Mechanisms exist to compel data and/or process owners to operationalize	5	
CC5.1-POF1	Integrates With Risk Assessment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Practices	GOV-15	cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
CC5.1-POF2	Considers Entity-Specific Factors	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	
CC5.1-POF2	Considers Entity-Specific Factors	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 & data privacy practices for each system, application and/or service under their control.	5	
CC5.1-POF3	Determines Relevant Business Processes	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 & data privacy practices for each system, application and/or service under their control.	5	
CC5.1-POF4	Evaluates a Mix of Control Activity Types	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 & data privacy practices for each system, application and/or service under their control.	5	
CC5.1-POF5	Considers at What Level Activities Are Applied	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 & data privacy practices for each system, application and/or service under their control.	5	
CC5.1-POF5	Considers at What Level Activities Are Applied	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Targeted Capability Maturity Levels Operationalizing	PRM-01.2	Mechanisms exist to define and identify targeted capability maturity levels.	5	
CC5.1-POF6	Addresses Segregation of Duties	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
CC5.1-POF6	Addresses Segregation of Duties	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.	5	
CC5.2	COSO Principle 11	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Privacy Portfolio Management Cybersecurity & Data	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy- related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives. Mechanisms exist to assess cybersecurity & data privacy controls in system project	5	
CC5.2	COSO Principle 11	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Privacy In Project Management	PRM-04	development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
CC5.2	COSO Principle 11	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
CC5.2	COSO Principle 11	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition		Mechanisms exist to define business processes with consideration for cybersecurity & data privacy the 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	
CC5.2	COSO Principle 11	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 systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
CC5.2	COSO Principle 11	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. Machanisms exist to conduct a Data Protection Impact Assessment (DRIA) on	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 systems, applications and services that store, process and/or transmit Personal Data (PDI 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 cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	5	



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	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
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 products and/or services 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	5	
CC5.2-POF1	Determines Dependency Between the Use of Technology in Business Processes and Technology General	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Asset-Service Dependencies	AST-01.1	based on applicable risks and threats. Mechanisms exist to identify and assess the security of technology assets that support more than one critical business function.	10	
CC5.2-POF2	Controls 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 systems, applications, services and third parties by graphically representing applicable boundaries.	5	
CC5.2-POF2	Establishes Relevant Technology Infrastructure Control Activities	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 & data privacy 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 a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
CC5.2-POF3	Establishes Relevant Security Management Process Controls	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	Activities 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 & 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 & 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 & data privacy 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 & 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 & data privacy principles into Business As Usual (BAU) practices through executive leadership involvement.	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	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
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	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	
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 secretic costs 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 VPM-02	Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and	5	
CC5.3-POF4	Performs Using Competent Personnel	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	Process Al & Autonomous Technologies Stakeholder Competencies	VPM-02 AAT-13.1	remediated. 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	
CC5.3-POF5	Performs Using Competent Personnel	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-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	Mechanisms exist to review the cybersecurity & data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy	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	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance. Mechanisms exist to facilitate the implementation of cryotographic protections	5	
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Use of Cryptographic Controls	CRY-01	controls using known public standards and trusted cryptographic technologies.	5	
CC6.1	N/A	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. Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	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	Encrypting Data At Rest Public Key Infrastructure	CRY-05	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	Mechanisms exist to facilitate cryptographic key management controls to protect the	5	
CC6.1	N/A	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	N/A	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	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identity & Access Management (IAM)	IAC-01	key. Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identification & Authentication for Non- Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5	
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.	5	
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identification & Authentication for Third Party Systems & Services	IAC-05	Mechanisms exist to identify and authenticate third-party systems and services.	5	
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Role-Based Access Control (RBAC) Identifier Management	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access. Mechanisms exist to govern naming standards for usernames and systems.	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	intersects with	(User Names) User Identity (ID)	IAC-09	Mechanisms exist to ensure proper user identification management for non-	5	
CU6.1	N/A	DOWNLOSE AICHA'S Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management	IAC-09.1	consumer users and administrators.	5	



Secure Controls Framework (SCF) 18 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)
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
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 creation or system installation.	5	
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Account Management Privileged Account	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system. service. application. guest and temporary accounts.	5	
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services. Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform	5	
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." Mechanisms exist to utilize the concept of least privilege, allowing only authorized	5	
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 organizational business functions.	5	
CC6.1	N/A	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	
CC6.1	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	intersects with	Boundary Protection Limit Network	NET-03 NET-03.1	boundary and at key internal boundaries within the network. Mechanisms exist to limit the number of concurrent external network connections to	5	
	N/A		Functional		Connections Data Flow Enforcement –	NET-04	its systems. Mechanisms exist to design, implement and review firewall and router	5	
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Access Control Lists (ACLs)	NE1-04	configurations to restrict connections between untrusted networks and internal systems. Mechanisms exist to prohibit the direct connection of a sensitive system to an	5	
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	External System Connections	NET-05.1	external network without the use of an organization-defined boundary protection device.	5	
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	
CC6.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security Management	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by	5	
	Identifies and Manages				Subnets		implementing separate subnetworks with managed interfaces to other components of the system. Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement		
CC6.1-POF1	the Inventory of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Asset Governance	AST-01	and manage asset management controls. Mechanisms exist to perform inventories of technology assets that:	10	
CC6.1-POF1	Identifies and Manages the Inventory of Information Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Asset Inventories	AST-02	(1) Accustately reflects the current systems, applications and services in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
CC6.1-POF1	Identifies and Manages the Inventory of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization	5	
000.110/1	Information Assets Identifies and Manages	DOWNLOOD AND A STATE CONTROL OF THE PROPERTY OF THE CONTROL TO THE CONTROL THE CONTROL TO THE CONTROL TO THE CONTROL TO THE CONTROL TO THE CO	Tunctional	mulacota with	Asset Scope Stassification	701 04.1	for all systems, applications, services and personnel (internal and third-parties). Mechanisms exist to ensure data and assets are categorized in accordance with	, and the second	
CC6.1-POF1	the Inventory of Information Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data & Asset Classification	DCH-02	applicable statutory, regulatory and contractual requirements.	5	
CC6.1-POF2	Assesses New Architectures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	
CC6.1-POF2	Assesses New Architectures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity & data privacy controls in systems, applications and services through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting exsected requirements.	5	
CC6.1-POF2	Assesses New Architectures	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 & data privacy practices in the specification, design, development,	5	
CC6.1-POF2	Assesses New Architectures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Alignment With Enterprise Architecture	SEA-02	Implementation and modification of systems and services. Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
CC6.1-POF3	Restricts Logical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
CC6.1-POF3	Restricts Logical Access	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	
CC6.1-POF3	Restricts Logical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
CC6.1-POF3	Restricts Logical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identification & Authentication for Non- Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5	
CC6.1-POF3	Restricts Logical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.	5	
CC6.1-POF4	Identifies and Authenticates Users	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	
CC6.1-POF4	Identifies and Authenticates Users	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
CC6.1-POF4	Identifies and Authenticates Users	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identification & Authentication for Non- Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5	
CC6.1-POF5	Considers Network Segmentation (macrosegementation)	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
CC6.1-POF5	Considers Network Segmentation (macrosegementation)	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cloud Access Security Broker (CASB)	CLD-11	Mechanisms exist to utilize a Cloud Access Security Broker (CASB), or similar 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	Considers Network Segmentation	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Network Security Controls (NSC)	NET-01	resources. Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
CC6.1-POF5	(macrosegementation) Considers Network Segmentation	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(NSC) Zero Trust Architecture	NET-01.1	Mechanisms exist to treat all users and devices as potential threats and prevent	5	
	(macrosegementation) Considers Network				(ZTA)		access to data and resources until the users can be properly authenticated and their access authorized. Mechanisms exist to monitor and control communications at the external network		
CC6.1-POF5	Segmentation (macrosegementation) Considers Network	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Boundary Protection	NET-03	boundary and at key internal boundaries within the network. Mechanisms exist to route all remote accesses through managed network access	5	
CC6.1-POF5	Segmentation (macrosegementation)	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Managed Access Control Points	NET-14.3	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 (ACLs)	NET-04	Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems.	5	
CC6.1-POF6	Manages Points of Access	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-POF7	Restricts Access to Information Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	System Hardening Through Baseline	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted	5	
CC6.1-POF7	Restricts Access to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configurations Least Functionality	CFG-03	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	
	Information Assets Restricts Access to				Identity & Access		specifically pronibiting or restricting the use of ports, protocols, and/or services. Mechanisms exist to facilitate the implementation of identification and access	,	
CC6.1-POF7	Information Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management (IAM)	IAC-01	management controls. Mechanisms exist to utilize the concept of least privilege, allowing only authorized	5	
CC6.1-POF7	Restricts Access to Information Assets	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 organizational business functions.	5	
CC6.1-POF8	Manages Identification and Authentication	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
CC6.1-POF8	Manages Identification and Authentication	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
		•	*				•		



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-POF8	Manages Identification and Authentication	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryotographically-based and replay resistant.	5	
CC6.1-POF8	Manages Identification and Authentication	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identification & Authentication for Third Party Systems & Services	IAC-05	Mechanisms exist to identify and authenticate third-party systems and services.	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	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
CC6.1-POF9	Manages Credentials for Infrastructure and	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	Software Manages Credentials for Infrastructure and	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 & data privacy assessment and authorization controls.	5	
CC6.1-POF9	Software Manages Credentials for Infrastructure and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security Authorization	IAO-07	Mechanisms exist to ensure systems, projects and services are officially authorized prior to "go live" in a production environment.	5	
CC6.1-POF10	Software 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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
CC6.1-POF10	Uses Encryption to Protect Data	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
CC6.1-POF10	Uses Encryption to Protect Data	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-POF10	Uses Encryption to Protect Data	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
CC6.1-POF10	Uses Encryption to Protect Data	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-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	Mechanisms exist to facilitate the production and management of asymmetric cryptographic keys using Federal Information Processing Standards (FIPS)- compliant key management technology and processes that protect the user's private key.	5	
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	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	Mechanisms exist to facilitate the production and management of asymmetric cryptographic keys using Federal Information Processing Standards (FIPS)- compliant key management technology and processes that protect the user's private key.	5	
CC6.1-POF11	Protects Cryptographic Keys	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5	
CC6.1-POF11	Protects Cryptographic Keys	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	5	
CC6.1-POF12	Restricts Access to and Use of Confidential	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 a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for	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	Access To Sensitive / Regulated Data	IAC-20.1	sensitive/regulated data access. 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 Purposes	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	
CC6.1-POF13	Restricts Access to and the Use of Personal Information	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 a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
CC6.1-POF13	Restricts Access to and the Use of Personal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Access To Sensitive / Regulated Data	IAC-20.1	Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.	5	
CC6.1-POF13	Information Restricts Access to and the Use of Personal Information	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	
CC6.1-POF13	Restricts Access to and the Use of Personal Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	5	
CC6.1-POF13	Restricts Access to and the Use of Personal Information	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	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 smount 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 unnecessary privileges, as necessary.	5	
CC6.2-POF1	Creates Access Credentials to Protected Information Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Provisioning & De- Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
CC6.2-POF1	Creates Access Credentials to Protected Information Assets	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-POF1	Creates Access Credentials to Protected Information Assets	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5	
CC6.2-POF2	Reviews Validity of Access Credentials	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-POF2	Reviews Validity of Access Credentials	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- defined time period.	5	
CC6.2-POF2	Reviews Validity of Access Credentials	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 cannot be associated with a business process and owner. Mechanisms exist to periodically-review the privileges assigned to individuals and	5	
CC6.2-POF2	Reviews Validity of Access Credentials Prevents the Use of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Periodic Review of Account Privileges	IAC-17	rechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary or hilleges, as necessary. Mechanisms exist to adjust togical and physical access authorizations to systems	5	
CC6.2-POF3	Credentials When No Longer Valid	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Personnel Transfer	HRS-08	and facilities upon personnel reassignment or transfer, in a timely manner.	5	
CC6.2-POF3	Prevents the Use of Credentials When No Prevents the Use of	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. Mechanisms exist to utilize a formal user registration and de-registration process	5	
CC6.2-POF3	Credentials When No Longer Valid Prevents the Use of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Provisioning & De- Provisioning	IAC-07	that governs the assignment of access rights. Mechanisms exist to review all system accounts and disable any account that	5	
CC6.2-POF3	Credentials When No Longer Valid Prevents the Use of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	System Account Reviews Periodic Review of	IAC-15.7	cannot be associated with a business process and owner. Mechanisms exist to periodically-review the privileges assigned to individuals and	5	
CC6.2-POF3	Credentials When No Longer Valid	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Account Privileges	IAC-17	service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
CC6.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for	10	
CC6.3-POF1	Creates or Modifies Access to Protected	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Provisioning & De- Provisioning	IAC-07	sensitive/regulated data access. Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
CC6.3-POF1	Creates or Modifies Access to Protected	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	
CC6.3-POF1	Information Assets Creates or Modifies Access to Protected	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5	
CC6.3-POF2	Removes Access to Protected Information	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Provisioning & De- Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
CC6.3-POF2	Removes Access to Protected Information	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	
CC6.3-POF3	Assets Uses Access Control Structures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for	10	
CC6.3-POF4	Reviews Access Roles and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Periodic Review of	IAC-17	sensitive/regulated data access. 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	
CC6.4	Rules N/A	Description of the second of t	Functional	intersects with	Account Privileges Physical & Environmental	PES-01	unnecessary privileges, as necessary. Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
		Download AICPA's Trust Services Criteria (TSC) for specific control wording.			Protections Physical Access		Physical access control mechanisms exist to maintain a current list of personnel		
CC6.4	N/A	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 facility officially designated as publicly accessible). Physical access control mechanisms exist to authorize physical access to facilities	5	
CC6.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Role-Based Physical Access	PES-02.1	based on the position or role of the individual. Physical access control mechanisms exist to enforce physical access authorizations	5	
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 (excluding those areas within the facility officially designated as publicly accessible).	5	
CC6.4-POF1	Creates or Modifies Physical Access	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	
CC6.4-POF1	Creates or Modifies Physical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
CC6.4-POF1	Creates or Modifies Physical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	5	
CC6.4-POF1	Creates or Modifies Physical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
CC6.4-POF2	,	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical & Environmental	PES-01	Mechanisms exist to facilitate the operation of physical and environmental	5	
					Protections		protection controls. Mechanisms exist to ensure visitor badges, or other issued identification, are		
CC6.4-POF2	Removes Physical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Visitor Access Revocation	PES-06.6	surrendered before visitors leave the facility or are deactivated at a pre-determined time/date of expiration. Physical access control mechanisms exist to maintain a current list of personnel	5	
CC6.4-POF2	Removes Physical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical Access Authorizations Role-Based Physical	PES-02	with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
CC6.4-POF2	Removes Physical Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual. Physical access control mechanisms exist to enforce physical access authorizations	5	
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 (excluding those areas within the facility officially designated as publicly accessible).	5	
CC6.4-POF3	Recovers Physical Devices	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Return of Assets	AST-10	Mechanisms exist to ensure that employees and third-party users return all organizational assets in their possession upon termination of employment, contract or agreement.	5	
CC6.4-POF3	Recovers Physical Devices	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. Physical access control mechanisms generate a log entry for each access attempt	5	
CC6.4-POF4	, , , , , , , , , , , , , , , , , , , ,	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 equal	Physical Access Logs Monitoring Physical	PES-03.3 PES-05	through controlled ingress and egress points. Physical access control mechanisms exist to monitor for, detect and respond to	10	
CC6.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Access Data Protection	DCH-01	physical security incidents. Mechanisms exist to facilitate the implementation of data protection controls.	10	
CC6.5	N/A	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	
CC6.5	N/A	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	5	
							formal procedures. Mechanisms exist to sanitize system media with the strength and integrity		
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 disposal, release out of organizational control or release for reuse. Mechanisms exist to securely dispose of, destroy or erase information.	5	
CC6.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Information Disposal	DCH-21	Mechanisms exist to:	5	
CC6.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Personal Data (PD) Retention & Disposal	PRI-05	(1) Retain Personal Data (PD), including metadats, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
CC6.5-POF1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	N/A	N/A	N/A	N/A	N/A Mechanisms exist to securely dispose of, destroy or repurpose system components	5	Removed from TSC 2017
CC6.5-POF2	Removes Data and Software for Disposal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	using organization-defined techniques and methods to prevent information being recovered from these components.	5	
CC6.5-POF2	Removes Data and Software for Disposal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
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 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 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 (ESP).	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	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC). Mechanisms exist to implement security functions as a layered structure that	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 tayered 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 Data Flow Enforcement –	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its systems. Mechanisms exist to design, implement and review firewall and router	5	
CC6.6	N/A	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.	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 (optional)	Notes (optional)
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).	(optional) 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, including 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	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network. Mechanisms exist to design, implement and review firewall and router	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	rectains as exist to clinique in evaluation of cryptographic protections	5	
CC6.6-POF2	Authentication Credentials Protects Identification and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Use of Cryptographic Controls	CRY-01	controls using known public standards and trusted cryptographic technologies. Mechanisms exist to facilitate the implementation of identification and access	5	
CC6.6-POF2	Authentication Credentials Protects Identification and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identity & Access Management (IAM)	IAC-01	management controls. Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit	5	
CC6.6-POF2	Authentication Credentials	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authenticate, Authorize and Audit (AAA)	IAC-01.2	(AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP). Mechanisms exist to enforce complexity, length and lifespan considerations to	5	
CC6.6-POF2	Authentication Credentials Protects Identification and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Password-Based Authentication	IAC-10.1	ensure strong criteria for password-based authentication. Mechanisms exist to develop, govern & update procedures to facilitate the	5	
CC6.6-POF2	Authentication Credentials Protects Identification and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Network Security Controls (NSC)	NET-01	recommisms exist to develop, govern a update procedures to factitate the implementation of Network Security Controls (NSC). Cryptographic mechanisms exist to implement strong cryptography and security	5	
CC6.6-POF2	Authentication Credentials Protects Identification and	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, oublic networks. Mechanisms exist to protect the confidentiality, integrity and availability of electronic	5	
CC6.6-POF2	Authentication Credentials Requires Additional	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Electronic Messaging Identity & Access	NET-13	recensisms exist to protect the confidentiality, integrity and availability of electronic messaging communications. Mechanisms exist to facilitate the implementation of identification and access	5	
CC6.6-POF3	Authentication or Requires Additional	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management (IAM)	IAC-01	management controls. Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit	5	
CC6.6-POF3	Authentication or Credentials	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Authenticate, Authorize and Audit (AAA)	IAC-01.2	(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	Mutti-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Tintri-party systems, applications and/or services; and/or (3) Non-console access to critical systems or systems 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 Credentials	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	Requires Additional Authentication or Credentials	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	Requires Additional Authentication or Credentials	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-POF3	Requires Additional Authentication or Credentials	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-POF4	Implements Boundary Protection Systems	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-POF4	Implements Boundary Protection Systems	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. Mechanisms exist to monitor and control communications at the external network	5	
CC6.6-POF4	Implements Boundary Protection Systems	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Boundary Protection	NET-03	boundary and at key internal boundaries within the network.	5	
CC6.6-POF4	Implements Boundary Protection Systems	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	
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	5	
CC6.7	N/A	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	
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	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. 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. Mechanisms exist to govern how external parties, systems and services are used to	5	
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Use of External Information Systems	DCH-13	Mechanisms exist to govern how external parties, systems and services are used to securely store, process and transmit data. Mechanisms exist to restrict or prohibit the use of portable storage devices by users	5	
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Portable Storage Devices	DCH-13.2		5	
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Information Sharing	DCH-14	decisions to ensure data is appropriately protected. Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or	5	
CC6.7	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Ad-Hoc Transfers Centralized Management	DCH-17	external parties. Mechanisms exist to implement and govern Mobile Device Management (MDM)	5	
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	Full Device & Container- 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 Restricts the Ability to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Electronic Messaging System Hardening	NET-13	messaging communications. Mechanisms exist to develop, document and maintain secure baseline	5	
CC6.7-POF1	Perform Transmission Restricts the Ability to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Through Baseline Configurations	CFG-02	configurations for technology platforms that are consistent with industry-accepted system hardening standards. Mechanisms exist to configure systems to provide only essential capabilities by	5	
CC6.7-POF1	Perform Transmission Restricts the Ability to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional Functional	intersects with	Least Functionality Ad-Hoc Transfers	CFG-03	specifically prohibiting or restricting the use of ports, protocols, and/or services. Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or	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	Prevent Unauthorized	DCH-17 NET-03.5	external parties. Automated mechanisms exist to prevent the unauthorized exfiltration of	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	intersects with	Exfiltration Deny Traffic by Default &	NET-04.1	sensitive/regulated data across managed interfaces. 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	
CC6.7-POF1	Perform Transmission Restricts the Ability to Perform Transmission	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Allow Traffic by Exception End-User Messaging Technologies	NET-12.2	exception). Mechanisms exist to prohibit the transmission of unprotected sensitive/regulated data by end-user messaging technologies.	5	
CC6.7-POF1	Restricts the Ability to Perform Transmission	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Loss Prevention (DLP)	NET-17	data by end-user messaging technologies. Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	



Secure Controls Framework (SCF) 22 of

Uses Encryption CC6.7-PDF2 Technologies or Secure CC6.7-PDF3 Protects Removal Media CC6.7-PDF4 Protects Remo	a being t of data at rest. t of controls. controls. t ocontrols. t	5	
Uses Encryption Technologies of Secure Communication: Channels Uses Encryption Technologies of Secure Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies of Secure Communication: Channels Uses Encryption Technologies of Secure Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies of Secure Communication: Channels Technologies of Secure Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies of Secure Communication: Channels Technologies of Secure Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies of Secure Technologies of Secure Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies of Secure Technologies of Secure Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies of Secure Technologies of Secure Technologies of Secure Technologies of Secure Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies of Secure	of data at rest. controls. intal distribution protections therefore, 1 of data at rest. intal distribution controls. intal distribution controls. intal distribution controls. intal distribution controls. interpretation inter	5 5 5 10 5 5 5	
CCB.7-POF3 Protects Removal Media CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria	racontrols. ! mal distribution protections 1	5 5 10 5 5 5	
CC6.7-PDF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies or Secure CC6.7-PDF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies or Secure CC6.7-PDF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies or Secure CC6.7-PDF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies or Secure CC6.7-PDF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies or Secure CC6.7-PDF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies or Secure Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies or Secure Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies or Secure Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies or Secure Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies Devices CC6.7-PDF4 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies Devices CC6.7-PDF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies Devices CC6.7-PDF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Technologies Devices CC6.7-PDF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific c	roontrois. Indistribution protections pro	5 5 10 5 5 5	
CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.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 are yield of sensitive-requisited media. Mechanisms exist to maintain strict control over the intermentation of cryptographic Control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devic	mat distribution ! protections theologies. 1 of information ! of data at rest. ! tatepity of tate handling and 1 tevices by users ! ty controls. ! ! ty controls. ! ! ! ! ! ! ! ! ! ! ! ! !	5 5 5 5	
CC6.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 P	protections theologies. 1 of information of data at rest. stegrity of sta handling and televices by users ity controls. ity controls. tenert (HDM)	5 5 5	
CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording	of information to of data at rest. thegrity of ata handling and tevices by users in controls. thent (MDM)	5 5 5	
CC6.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific	of data at rest.	5	
CCB.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.7-POF4 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Portable Storage Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with English Storage Devices CCB.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Control wording. Functional Intersects with Portable Storage Devices AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Portable Storage Devices AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Portable Storage Devices AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Portable Storage Devices AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Portable Storage Devices AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Portable Storage Devices AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Portable Storage Devices AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Portable Storage Devices AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Portable Storage Devices AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Portable Storage Devices AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Portabl	sta handling and 1 levices by users 1 ity controls. 1 nent (MDM) 1	10	
CC6.7-POF3 Protects Removal Media Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Empoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Empoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Empoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Empoint Security Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Probability of Control wording Criteria (TSC) for specific control wording. Functional Intersects with Probability of Control wording Criteria (TSC) for specific control wording. Functional Intersects with Probability of Criteria (TSC) for specific control wording. Functional Intersects with Probability of Control wording (Criteria (TSC) for specific control wording. Functional Intersects with Probability of Changes Criteria (TSC) for specific control wording. Functional Intersects with Probability of Changes Criteria (TSC) for specific control wording. Functional Intersects with Probability of Changes Criteria (TSC) for specific control wording. Functional Intersects with Probability of Changes Criteria (TSC) for specific control wording. Functional Intersects with Probability of Changes Criteria (TSC) for specific control wording. Functional Intersects with Probability of Changes Criteria (TSC) for specific control wording. Functional Intersects with Probability of Changes Criteria (TSC) for specific control wording. Functional Intersects with Probability of Changes Criteria (TSC) for specific control wording. Functional Intersects with Probability of Changes Criteria (TSC) for specific control wording. Functional Intersects with Probability of Changes Criteria (TSC) for speci	levices by users		
CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. CC6.7-POF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Controllad Management Of Mobile Devices Model of CPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Controllad Management Of Mobile Devices Model of CPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for specific control wording. Functional Intersects with Prohibition Of Chinages Criteria (TSC) for speci	rity controls.	5	
CC6.7-PCF4 Protects Endpoint Devices Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Centralized Management Of Mobile Devices NA Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Prohibition Of Changes Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Criteria with Criteria (TSC) for specific control wording. Functional intersects with Criteria with Crite	nent (MDM)	_	
CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Prohibition Cf Changes CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection (n/in-Malware) (n/in-Malware) CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection (n/in-Malware) CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection (n/in-Malware) CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection (n/in-Malware) CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection (n/in-Malware) CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection (n/in-Malware) CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection (n/in-Malware) CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection (n/in-Malware) CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection (n/in-Malware) CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection (n/in-Malware) CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection (n/in-Malware) CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection (n/in-Malware) CC6.8 N/A Download AI			
CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Malicious Code Protection (Anth-Makware) END-04 malicious code. Mechanisms exist to utilize antimalware technologies to detect and malicious code. Mechanisms exist to utilize antimalware technologies to detect and malicious code. END-04 malicious code. End-of-int File linegity END-04 End-ont File linegity END-04 END-04 END-04 File Integrity Monitor (FM), or similar technologies to detect and malicious code.			
(Anti-Malware) (Anti-Malware)			
		5	
Monitoring (FIM) Monitoring (FIM)	figuration	5	
CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with intersects with a Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with intersects with an Prevention Systems (HUDS / HIPS) without technologies, to monitor for and protect age 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) (FIM		5	
CC6.8 N/A Download A/CPA'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 exhaust.	ternal network	5	
CC6.8 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Detection / Prevention Mechanisms exist to employ Network Instrusion Mechanisms exist to		5	
Restricts installation and Modification of Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with User-installated Software. Systems (NIDS / NIPS) Mechanisms exist to restrict the ability of non-privileged users to in unsurfaced software.		5	
Application and Software Restricts Installation and Modification of Modificat		5	
Application and Software Restricts Installation and CC6.8-POF1 Modification of Modification of Download AICPA's Trust Services Oriteria (TSC) for specific control wording. Functional intersects with Methods for the Modification of Download AICPA's Trust Services Oriteria (TSC) for specific control wording. Functional intersects with Methods for the Modification of Download AICPA's Trust Services Oriteria (TSC) for specific control wording. Functional intersects with Methods for the Modification of Download AICPA's Trust Services Oriteria (TSC) for specific control wording.		5	
Application and Software Detects Unauthorized CC6.8-POF2 Changes to Software and Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Intersects with Alerts	e unauthorized	5	
Confluention Parameters Detects Unantiforized Changes to Software and Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Intersects with Alerts Alerts Alerts Alerts	d.	5	
Configuration Parameters CE.8.POF3 Use a Defined Change Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Program Prog	agement t	5	
CC6.8-PGF3 Uses Defined Change Control Process Control Process Control AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Control		5	
CC6.8-POF4 Uses Antivirus and Anti-Malware Software Malvare Software Download AICPA's Trust Services Oriteria (TSC) for specific control wording. Functional equal Malicious Code Protection (Anti-Malware) END-04 Malicious Code Protection (Anti-Malware)		10	
Scans Information Assets From Outside the Entity Tor Malware and Other Unauthorized Software Unauthorized Soft	ged users,	10	
CC7.1 N/A Download AICPA's Trust Services Oriteria (TSC) for specific control wording. Functional intersects with Management Program Management Program CFG-01		5	
CC7.1 N/A Download AICPA's Trust Services Oriteria (TSC) for specific control wording. Functional intersects with incomplete and the specific control wording intersects with incomplete and the specific control wording. System Hardening Configurations for technology platforms that are consistent with incomplete and the specific control wording and standards.		5	
CC7.1 N/A Download AICPA's Trust Services Oriteria (TSC) for specific control wording. Functional intersects with Integrity Checks END-66.1 and firmware.		G.	
CC7.1 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with (RIM) (RIM) MON-01.7 (Exchanging exist to utilize a File Integrity Monitor (FIM), or similar (RIM) MON-01.7 technology, on critical assets to generate alerts for unauthorized monitorized monitoring (RIM) (RIM) MON-01.7 technology, on critical assets to generate alerts for unauthorized monitorized monitoring (RIM) (RI	hange-detection difications.	5	
CC7.1 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Vulnerability Scanning VPM-06 vulnerability scanning of systems and applications.		5	
CC7.1-POF1 Uses Defined Configuration Sandards Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Management Program Management Program CFG-01 Mechanisms exist to facilitate the implementation of configuration controls.	nanagement	5	
CC7.1-POF1 Uses Defined Configuration Sandards Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Function		5	
CC7.1-POF1 Configuration Sandards. CC7.1-POF1 Configuration Sandards. Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Management & GF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM), or CF-02.2 systems through Continuous Diagnostics and Mitigation (CDM).		5	
CC7.1-PGF2 Monitors Infrastructure and Software and Softw		5	
CC7.1-POF2 Monitors Infrastructure and Software and Soft		5	
CC7.1-POF3 Implements Change-Detection Mechanisms Download AICPA's Trust Services Oriteria (TSC) for specific control wording. Functional intersects with Intersects with Monitoring (FIM) Mechanisms exist to utilize File Integrity Monitor (FIM), or similar teaching file of the Integrity Monitoring (FIM) Mechanisms exist to utilize File Integrity Monitor (FIM), or similar teaching file or selected files and constitutions.		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 of technology, on critical assets to generate alerts for unauthorized minimum.	difications.	5	
Detects Unknown or Louise Development Detector Unknown or Louise Development Detector CC7.1-POF4 Development Detector Components Detector Development Detector Component Detector Development		5	
Detects Unknown or CC7.1-POF4 Unsurbridged Components Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Functional Intersects with Monitoring (FIM) END-65 detect and report on unauthorized changes to selected files and control wording. END-65 settines.	figuration	5	
Detects Unknown or Unsurbnized Components Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with File Integrity Monitoring (FIM) MON-01.7 (FIM) MON-01.7 (MIX) Monitoring (FIM) MON-01.7 (MIX) Monitoring (FIM)		5	
CC7.1-POFS Conducts Vulnerability Scenning Security Secur	1	10	
CC7.2 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Management & CFG-02 2 systems through Continuous Diagnostics and Mitigation (CDM), or 1 technologies.	imilar	5	
CC7.2 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Continuous Monitoring MON-91 (MON-91)		5	
CC7.2 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intrusion Detection & Mechanisms exist to implement intrusion Detection A prevention Systems (IDS & MON-31). technologies on critical systems, IDS & MON-31. Technologies on critical systems (IDS & Mon-31. Technologies on critical systems, IDS & Mon-31. Technologies on	k choke points.	5	
CC7.2 N/A Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Intersects with Intersects with Automated Tools for Real-Time Analysis Automated Tools for Real-Time Analysis MON-01.2 automated tool, to support near real-time analysis and incident esci		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	Notes (optional)
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	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	(optional) 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	5	
CC7.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Wireless Intrusion	MON-01 F	situational awareness. Mechanisms exist to utilize Wireless Intrusion Detection / Protection Systems (WIDS 5 / VMPS) to Identify rogue wireless devices and to detect attack attempts via wireless	5	
					Detection System (WIDS)		networks. Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems	-	
CC7.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Host-Based Devices	MON-01.6	[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. Mechanisms exist to review event logs on an ongoing basis and escalate incidents in	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	accordance with established timelines and procedures. Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar	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	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 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	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 & 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		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	assigned daks.	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 alerts 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 anomatous 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 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 & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
CC7.2-POF3	Implements Filters to Analyze Anomalies	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-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 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 Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	
CC7.2-POF4	Monitors Detection Tools for Effective Operation	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	
CC7.3	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 & data privacy- related incidents. Mechanisms exist to cover:	5	
CC7.3	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) Analysie; (4) Containment; (5) Endication; 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		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	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 systems and data.	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	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 & data privacy-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;	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	Mechanisms exist to maintain and make available a current and viable incident Response Plan (IRP) to all stakeholders.	5	
CC7.3-POF2	Communicates and Reviews Detected Security Events	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 & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	5	
	LYONG								



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 (optional)	Notes (optional)
CC7.3-POF2	Communicates and Reviews Detected Security Events	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	
CC7.3-POF2	Communicates and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	(3) Regulatory authorities. Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
CC7.3-POF3	Events 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) Endication; and (6) Renower.	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	(4) Containment; (5) Eradication; and (6) Recovery	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 awant detection or manual incident report intoke:	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:	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 effecting 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	Determines Personal 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; L2) automated exent detection or manual incident report intake:	5	
CC7.3-POF7	Determines Personal 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		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 & data privacy- related incidents.	5	
CC7.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	(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) Integrated Security	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders. Mechanisms exist to establish an integrated team of cybersecurity, IT and business	5	
CC7.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Team (ISIRT)	IRO-07	function representatives that are capable of addressing cybersecurity & data privacy incident resoonse operations. Mechanisms exist to document, monitor and report the status of cybersecurity &	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	data privacy incidents to internal stakeholders all the way through the resolution of the incident. Mechanisms exist to timely-report incidents to applicable:	5	
CC7.4	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	
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	Machanisms aviet to report consists (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	Supply Chain Coordination Coordination With	IRO-10.4	provider of the product or service and other organizations involved in the supply chain for systems or system components related to the incident.	5	
CC7.4	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	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 Risk Remediation	RSK-06	and law enforcement agencies. Mechanisms exist to remediate risks to an acceptable level.	5	
CC7.4-POF1	Assigns Roles and Responsibilities	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 $\pmb{\delta}$ responsibilities for all personnel.	5	
CC7.4-POF1	Assigns Roles and Responsibilities	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 & data privacy-	5	
CC7.4-POF1	Assigns Roles and Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	related incidents. Mechanisms exist to cover: (1) Preparation;	5	
CC7.4-POF1	Assigns Roles and Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	I'll Automated exent dataction or manual incident caport inteize: Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
CC7.4-POF1	Assigns Roles and Responsibilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Integrated Security Incident Response Team	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy	5	
CC7.4-POF2	Contains and Responds to Security Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(ISIRT) Incident Response Operations	IRO-01	Incident response operations. Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-	5	
CC7.4-POF2	Contains and Responds to Security Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	(4) Containment; (5) Eradication; and	5	
CC7.4-POF2	Contains and Responds to Security Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	IBI Recovery Mechanisms exist to maintain and make available a current and viable incident Response Plan (IRP) to all stakeholders.	5	
CC7.4-POF3	Mitigates Ongoing 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 & data privacy- related incidents.	5	
CC7.4-POF3	Mitigates Ongoing 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; (6) Endication; and	5	
CC7.4-POF3	Mitigates Ongoing Security Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	(6) Recruenz Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
CC7.4-POF4	Resolves 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 & data privacy-related incidents.	5	
CC7.4-POF4	Resolves 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; (6) Eradication; and	5	
CC7.4-POF4	Resolves 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	
CC7.4-POF5	Restores Operations	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 assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
CC7.4-POF5	Restores Operations	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 & data privacy-related incidents.	5	
	1	1	1	1	1	1	related incidents.	1	I.



Secure Controls Framework (SCF) 25 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)
CC7.4-POF5	Restores Operations	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;	(optional) 5	
007.4 POFF	Bastona Occasiona	Description (ICDN) To the Control of College (ICDN) to the ICDN (ICDN)	Functional		Incident Response Plan	IRO-04	(5) Eradication; and (6) Recovery Mechanisms exist to maintain and make available a current and viable incident	-	
CC7.4-POF5	Restores Operations Develops and Implements	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	(IRP) Incident Response	IRO-04	Response Plan (IRP) to all stakeholders. Mechanisms exist to implement and govern processes and documentation to	5	
	Communication of Security Incidents Develops and Implements				Operations		facilitate an organization-wide response capability for cybersecurity & data privacy- related incidents. Mechanisms exist to cover:		
CC7.4-POF6	Communication of Security Incidents Develops and Implements	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling Incident Response Plan	IRO-02	(1) Preparation; (2) Automated event detection or manual incident report intake: Mechanisms exist to maintain and make available a current and viable incident	5	
CC7.4-POF6	Communication of Security Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(IRP)	IRO-04	Response Plan (IRP) to all stakeholders. Mechanisms exist to document, monitor and report the status of cybersecurity &	5	
CC7.4-POF6	Security Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Situational Awareness For Incidents	IRO-09	data privacy incidents to internal stakeholders all the way through the resolution of the incident. Mechanisms exist to timely-report incidents to applicable:	5	
CC7.4-POF6	Develops and Implements Communication of Security Incidents Develops and Implements	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. Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
CC7.4-POF6	Communication of Security Incidents	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-POF7	Obtains Understanding of Nature of Incident and Determines Containment Strategy	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 tacilitate an organization-wide response capability for cybersecurity & data privacy- related incidents.	5	
CC7.4-POF7	Obtains Understanding of Nature of Incident and Determines Containment 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;	5	
CC7.4-POF7	Obtains Understanding of Nature of Incident and Determines 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-POF8	Remediates Identified Vulnerabilities	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 & data privacy-	5	
CC7.4-POF8	Remediates Identified Vulnerabilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	related incidents. Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (6) Eradication; and	5	
CC7.4-POF8	Remediates Identified Vulnerabilities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	ISI Rennverv Mechanisms exist to maintain and make available a current and viable incident Response Plan (RP) to all stakeholders.	5	
CC7.4-POF8	Remediates Identified Vulnerabilities Remediates Identified	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	
CC7.4-POF8	Vulnerabilities Communicates	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Process Incident Response	VPM-02	remediated. Mechanisms exist to implement and govern processes and documentation to	5	
CC7.4-POF9	Remediation Activities	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 & data privacy- related incidents. Mechanisms exist to cover:	5	
CC7.4-POF9	Communicates Remediation Activities	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;	5	
CC7.4-POF9	Communicates Remediation Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Plan	IRO-04	(6) Recovery Mechanisms exist to maintain and make svailable a current and viable incident Response Plan (IRP) to all stakeholders.	5	
CC7.4-POF9	Communicates Remediation 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 & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	5	
CC7.4-POF9	Communicates Remediation 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	Evaluates the Effectiveness of Incident Response	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	
CC7.4-POF10	Evaluates the	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 & data privacy-	5	
CC7.4-POF10	Evaluates the	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Handling	IRO-02	related incidents. Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (8) Recovery.	5	
CC7.4-POF10	Evaluates the Effectiveness of Incident	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-POF10		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 & data privacy incidents to reduce the likelihood or impact of future	5	
CC7.4-POF11	Response Periodically Evaluates Incidents	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Operations	IRO-01	Incidents. Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-	5	
CC7.4-POF11	Periodically Evaluates	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Operations Incident Handling	IRO-02	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	(1) Preparation; (1) Automated award detection or manual incident report intake: Mechanisms exist to maintain and make availtable a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
CC7.4-POF11	Incidents Periodically Evaluates		Functional	intersects with	(IRP)	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to	5	
	Incidents Applies Breach Response	Download AICPA's Trust Services Criteria (TSC) for specific control wording.			IRP Update		incorporate lessons learned, business process changes and industry developments, as necessary. Mechanisms exist to implement and govern processes and documentation to		
CC7.4-POF12	Applies Breach Response Procedures	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	Operations Incident Handling	IRO-01	facilitate an organization-wide response capability for cybersecurity & data privacy- related incident. Mechanisms exist to cover: (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	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	5	
CC7.4-POF13	Procedures Communicates Unauthorized Use and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(IRP) Incident Response Operations	IRO-01	Response Plan (IRP) to all stakeholders. Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-	5	
CC7.4-POF13	Disclosure Communicates	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Operations Incident Handling	IRO-02	related incidents. Mechanisms exist to cover: (1) Preparation;	5	
CC7.4-POF13	Disclosure Communicates	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Response Plan	IRO-04	(2) Automated event detection or manual incident report intake: Mechanisms exist to maintain and make available a current and viable Incident	5	
CC7.4-POF13	Disclosure Communicates Unauthorized Use and	Download AICPA's Trust Services Criteria (ISC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(IRP) Incident Stakeholder Reporting	IRO-10	Response Plan (IRP) to all stakeholders. Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected (Joint & Mirch parlies: and	5	
	Disclosure Communicates				Reporting Cyber Incident Reporting		(2) Affected clients & third-parties; and (3) Regulatory authorities. Mechanisms exist to report sensitive/regulated data incidents in a timely manner.		
CC7.4-POF14	Unauthorized Use and Disclosure Application of Sanctions	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	for Sensitive Data	IRO-10.2	Mechanisms exist to sanction personnel failing to comply with established security	5	
CC7.4-POF14	Appucation of Sanctions	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Personnel Sanctions	HRS-07	policies, standards and procedures.	10	



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 (optional)	Notes (optional)
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-0	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Identify Critical Assets	BCD-0	Mechanisms exist to identify and document the critical systems, applications and services 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	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	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Continue Essential Mission & Business Functions	BCD-02	Mechanisms exist to continue essential missions and business functions with little 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	Resume Essential Missions & Business	BCD-02	Mechanisms exist to resume essential missions and business functions within an	5	
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Functions Contingency Plan Testing & Exercises	BCD-0	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency Joan'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) &	BCD-0	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "tessons learned" 5 activity every time the contingency plan is activated.	5	
					Lessons Learned		Mechanisms exist to update contingency plans due to changes affecting:		
							 People (e.g., personnel changes); Processes (e.g., new, attered or decommissioned business practices, including third-party services) 		
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Ongoing Contingency Planning	BCD-0	(4) Data (e.g., changes to data flows and/or data repositories);	5	
							(5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or(6) Feedback from contingency plan testing activities.		
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Backups	BCD-1	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	5	
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Testing for Reliability &	BCD-11	the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Mechanisms exist to routinely test backups that verify the reliability of the backup	5	
CC7.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Integrity Information System	BCD-1	process, as well as the integrity and availability of the data. Mechanisms exist to ensure the secure recovery and reconstitution of systems 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	Recovery & Reconstitution Backup & Restoration	BCD-1	M. de al control de la control	5	
	Restores the Affected				Hardware Protection Business Continuity		Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan		
CC7.5-POF1	Environment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Management System (BCMS)	BCD-0	(COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	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	0.01	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	Mechanisms exist to continue essential missions and business functions with little 2.2 or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites.	5	
CC7.5-POF1	Restores the Affected Environment	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Resume Essential Missions & Business	BCD-02	Mechanisms exist to resume essential missions and business functions within an	5	
CC7.5-POF1	Restores the Affected	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Functions Information System	BCD-1	Mechanisms exist to ensure the secure recovery and reconstitution of systems to a known state after a disruption, compromise or failure.	5	
	Environment Communicates				Recovery & Reconstitution Business Continuity		Mechanisms exist to facilitate the implementation of contingency planning controls		
CC7.5-POF2	Incident	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Management System (BCMS)	BCD-0	(COOP) or Business Continuity & Disaster Recovery (BC/DR) 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	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	Communicates Information About the	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Incident Stakeholder	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders;	5	
	Incident Determines Root Cause of				Reporting Contingency Plan Root		(2) Affected clients & third-parties; and (3) Regulatory authorities. Mechanisms exist to conduct a Root Cause Analysis (RCA) and "tessons learned"		
CC7.5-POF3	the Incident	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Cause Analysis (RCA) & Lessons Learned	BCD-0	5 activity every time the contingency plan is activated. Mechanisms exist to facilitate the implementation of contingency planning controls	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-0	to help eneura reciliant accets and carriose (a.g. Continuity of Operations Plan	5	
							Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes);		
CC7.5-POF4	Implements Changes to Prevent and Detect	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Ongoing Contingency	BCD-0	[2] Processes (e.g., new, attered or decommissioned business practices, including third-party services) [5] (3) Technologies (e.g., new, attered or decommissioned technologies);	5	
	Recurrences				Planning		(4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, sitered or decommissioned physical infrastructure); and/or		
					Business Continuity		(6) Feedback from contingency plan testing activities. Mechanisms exist to facilitate the implementation of contingency planning controls		
CC7.5-POF5	Improves Response and Recovery Procedures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management System (BCMS)	BCD-0	to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
							Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes);		
CC7.5-POF5	Improves Response and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Ongoing Contingency	BCD-0	[2] Processes (e.g., new, altered or decommissioned business practices, including third-party services) [5] (3) Technologies (e.g., new, altered or decommissioned technologies);	5	
	Recovery Procedures				Planning		(4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or		
	Implements Incident-				Contingency Plan Testing		(6) Feedback from contingency plan testing activities. Mechanisms exist to conduct tests and/or exercises to evaluate the contingency	-	
CC7.5-POF6	Recovery Plan Testing	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	& Exercises System Hardening	BCD-0	plan's effectiveness and the organization's readiness to execute the plan. Mechanisms exist to develop, document and maintain secure baseline	10	
CC8.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Through Baseline Configurations	CFG-02	2 configurations for technology platforms 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	(2) When required due to so; or	5	
CC8.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Automated Central Management &	CFG-02	(3) As part of system component installations and upgrades. Automated mechanisms exist to govern and report on basine configurations of 22 systems through Continuous Diagnostics and Mitigation (CDM), or similar	5	
CC8.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Verification Change Management	CHG-0	technologies. Mechanisms exist to facilitate the implementation of a change management	5	
CC8.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Program Configuration Change Control	CHG-0	program. Mechanisms eviat to govern the technical configuration change control processes.	5	
CC8.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Test, Validate & Document Changes	CHG-02	F	5	
CC8.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Stakeholder Notification of Changes	CHG-0	environment. Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5	
CC8.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-0	Mechanisms exist to ensure changes to systems within the Secure Development Life	5	
CC8.1-POF1	Manages Changes Throughout the System	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change Management Program	CHG-0	Mechanisms exist to facilitate the implementation of a change management program.	5	
CC8.1-POF1	Life Cycle Manages Changes Throughout the System	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Change Control	CHG-0	Mechanisms exist to govern the technical configuration change control processes.	5	
CC8.1-POF1	Life Cycle Manages Changes Throughout the System	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Development Life Cycle (SDLC)	PRM-0	Mechanisms exist to ensure changes to systems within the Secure Development Llfe Cycle (SDLC) are controlled through formal change control procedures.	e 5	
CC8.1-POF2	Life Cycle Authorizes Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management Change Management	CHG-0	Mechanisms exist to facilitate the implementation of a change management	5	
CC8.1-POF2	Authorizes Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Program Configuration Change Control	CHG-0		5	
CC8.1-POF2	Authorizes Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Prohibition Of Changes Access Restriction For	CHG-02	change requests are received. Mechanisms exist to enforce configuration restrictions in an effort to restrict the	5	
CC8.1-POF2	Authorizes Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change	CHG-0	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	



cure Controls Framework (SCF) 27 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)
	CC8.1-POF3		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CHG-01		(optional) 5	
	CC8.1-POF3	Designs and Develops	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Change	CHG-02		5	
March Marc	CC8 1-POF3		Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	intersects with		CHG-02.3		5	
Description		-				Asset Lifecycle Changes				
March Marc		Changes				for Changes		to the implementation of the change.		
Part				-		Program		program.		
						Control				
March Marc	CC8.1-POF4	Documents Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Changes	CHG-02.2	environment.	5	
Manufacture						Program		program.		
Control Cont						Control				
Column	CC8.1-POF5	Tracks System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Changes	CHG-02.2	environment.	5	
1999 1999		-				Program		program.		
March Marc		-				Control				
Col. No. Col. C		Configures Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management Program	CFG-01	controls.	5	
Col. 1975	CC8.1-POF6	Configures Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configurations	CFG-02	system hardening standards.	5	
Column	CC8.1-POF6	Configures Software	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management &	CFG-02.2	systems through Continuous Diagnostics and Mitigation (CDM), or similar	5	
Page	0004 0057	Total Control Character	Desired Alonal Test of Colors (TOO) (1-1-1-1)	Frankland.			0110.04	Mechanisms exist to facilitate the implementation of a change management	-	
State Company Compan	CC8.1-POF7	Tests System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Program	CHG-01		5	
Col.	CC8.1-POF7	Tests System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
Col. 1979 Col. 1970						Control		Mechanisms exist to appropriately test and document proposed changes in a non-		
Section Sect	CC8.1-POF7	Tests System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CHG-02.2		5	
Section Control Cont	CC8.1-POF8	Approves System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of		CHG-01		10	
CSA 1995	CC8.1-POF8	Approves System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Configuration Change	CHG-02		10	
Col. 1-707	CC8.1-POF9	Deploys System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CHG-01		5	
Col. 1-1976 Pumps Spenis Obuse Section (Col. 1) Col. 1-1976 Pumps Spenis Obuse Section (Co	CC8 1 BOE0	Donlaus Sustam Changes	Download AICDA's Trust Sanions Criteria (TSC) for appoint a control wording	Eupational	interposts with	Configuration Change	CHC 03	Mechanisms exist to govern the technical configuration change control processes.	-	
Cold Total Cold	CC8.1-POF9	Deploys System Changes	Download AICPA'S Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CHG-02	Mechanisms exist to enforce configuration restrictions in an effort to restrict the	•	
Col. 1971 Col.	CC8.1-POF9	Deploys System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change	CHG-04		5	
Column C	CC8.1-POF9	Deploys System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Implement Changes	CHG-04.4		5	
Col. 1979 Section Company Section Col. 1979 Section Col. 1	CC8.1-POF10		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CHG-01		5	
Cot 1797	CC8.1-POF10		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
COS. 1679 1 Service and Travelle Control and Control and Cost (Cost Incomplete Cost Incomplete	CC8.1-POF10		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CHG-02.2		5	
South Colleges Cost 1970 South Colleges Cost 1970 South Colleges Cost 1971 So	CC8 1-POF10		Download AICPA's Trust Sanicas Critaria (TSC) for specific control wording	Functional	intercepts with	-	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior	5	
South Chapter Services Chapters Services Chapter Services						_		* * * * * * * * * * * * * * * * * * * *		
Col. 1-POF1 Internation District And Privation District And Pri	CC8.1-POF10	System Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Enforcement / Auditing	CHG-04.1		5	
Section 1.	CC8.1-POF11	Infrastructure, Data,	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CHG-01		5	
COL 1-POT 12 COL 1-POT 12 COL 1-POT 13 COL 1-POT 13 COL 1-POT 14 COL 1-POT 15 COL 1	CC8.1-POF11	Identifies Changes in Infrastructure, Data,	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
Software and Procedure Cost 1971 Cost 1971	CC8 1-POF11	Identifies Changes in	Download AICPA's Trust Sandres Criteria (TSC) for enacific control wording	Functional	intersects with	Automated Access	CHG-M 1		5	
Inflamorutus Districts Dis	550.115/11	Software, and Procedures Identifies Changes in	DOWNSON AS TRACES TOOS O'RETTA (1997) OF SPECIAL COURSE WORKING.	Tunctional	mulacota with	Enforcement / Auditing	0110 04.1		-	
Cold Fig. 1 Processing Pr	CC8.1-POF11	Software, and Procedures	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management &	CFG-02.2	systems through Continuous Diagnostics and Mitigation (CDM), or similar	5	
COL 1970 12 Contract Building Country of Cou		Incidents						Market and the state of the sta		
CCS FP0*12 Configuration of IT Demokrack APPA Trust Services Criteria (TSC) for specific control wording. CCS FP0*13 Receives in Emergency Demokrack APPA Trust Services Criteria (TSC) for specific control wording. CCS FP0*13 Receives in Emergency Demokrack APPA Trust Services Criteria (TSC) for specific control wording. CCS FP0*13 Receives in Emergency Demokrack APPA Trust Services Criteria (TSC) for specific control wording. CCS FP0*13 Receives in Emergency Demokrack APPA Trust Services Criteria (TSC) for specific control wording. CCS FP0*14 Receives in Emergency Demokrack APPA Trust Services Criteria (TSC) for specific control wording. CCS FP0*15 Receives in Emergency Demokrack APPA Trust Services Criteria (TSC) for specific control wording. CCS FP0*14 Receives in Emergency Demokrack APPA Trust Services Criteria (TSC) for specific control wording. CCS FP0*14 Receives in Emergency Demokrack APPA Trust Services Criteria (TSC) for specific control wording. CCS FP0*14 Receives in Emergency Demokrack APPA Trust Services Criteria (TSC) for specific control wording. CCS FP0*14 Receives in Emergency Demokrack APPA Trust Services Criteria (TSC) for specific control wording. CCS FP0*14 Receives in Emergency Demokrack APPA Trust Services Criteria (TSC) for specific control wording. CCS FP0*14 Receives in Emergency Demokrack APPA Trust Services Criteria (TSC) for specific control wording. CCS FP0*15 Receives in Emergency Demokrack APPA Trust Services Criteria (TSC) for specific control wording. CCS FP0*14 Receives in Emergency Demokrack APPA Trust Services Criteria (TSC) for specific control wording. CCS FP0*15 Receives Service Services Criteria (TSC) for specific control wording. CCS FP0*16 Receives Services Criteria (TSC) for specific control wording. CCS FP0*16 Prices Confidents Services Criteria (TSC) for specific control wording. CCS FP0*16 Prices Confidents Services Criteria (TSC) for specific control wording. CCS FP0*16 Prices Confidents Services Confidents Services Criteria (TSC) for specific c	CC8.1-POF12	Configuration of IT	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management Program	CFG-01	controls.	5	
Necessary in Emergency Description Descr	CC8.1-POF12	Configuration of IT Technology	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Through Baseline	CFG-02	configurations for technology platforms that are consistent with industry-accepted	5	
CCEL-POF13 Necessary in Temperation Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF14 Necessary in Temperation Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF15 Necessary in Temperation Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF16 Necessary in Temperation Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF16 Necessary in Temperation Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF16 Necessary in Temperation Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF16 Necessary in Temperation Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF16 Necessary in Temperation Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF16 Necessary in Temperation Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF16 Necessary in Temperation Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF16 Necessary in Temperation Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF17 Necessary in Temperation Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF18 Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF18 Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF18 Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF18 Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF18 Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF18 Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF18 Developed ACPA's Trust Services Criteria (TSC) for specific control wording. CCEL-POF18 Protects Contributed Necessary Services Cont	CC8.1-POF13	Provides for Changes Necessary in Emergency	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Change Management	CHG-01	Mechanisms exist to facilitate the implementation of a change management	5	
CCS.1-POF13 Nocessary in Emergency Ocolerated North Changes Nocessary in Emergency CCS.1-POF13 Nocessary in Emergency CCS.1-POF13 Nocessary in Emergency CCS.1-POF13 Nocessary in Emergency CCS.1-POF14 Nocessary in Emergency CCS.1-POF15 Nocessary in Emergency CCS.1-POF15 Nocessary in Emergency CCS.1-POF15 Nocessary in Emergency CCS.1-POF15 Nocessary in Emergency CCS.1-POF16 Nocessary in Emergency CCS	CC8.1-POF13	Provides for Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Configuration Change	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
CCB.1-PDF13 Necessay in Emergency COB.1-PDF13 Necessay in Emergency COB.1-PDF13 Necessay in Emergency COB.1-PDF13 Necessay in Emergency COB.1-PDF14 Nergency Potentials COB.1-PDF15 Nergency Potentials COB.1-PDF15 Nergency Potentials COB.1-PDF15 Nergency Potentials COB.1-PDF16 Potenti		Situations Provides for Changes								
CCB.1-POF13 Nessary in Emergency Accounts State Processory in Emergency Accounts State Processor State Process	CC8.1-POF13	Situations	Downtoad ArCPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CHG-02.2	environment.	5	
CCB.1-POF14 Manages Patch Changes Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.1-POF14 Manages Patch Changes Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Management Program CCB.1-POF15 Considers System Resilience CCB.1-POF15 Considers System Resilience CCB.1-POF16 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Management Program CCB.1-POF16 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Management Program CCB.1-POF16 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Management Program CCB.1-POF16 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Management Program CCB.1-POF16 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Management Program CCB.1-POF16 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Secure Engineering Principies CCB.1-POF16 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Principies CCB.1-POF16 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Properties Control wording. Functional intersects with Prop	CC8.1-POF13		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		IAC-15.9		5	
CCB.1-POF14 Manages Patch Changes Download AICPA's Trust Services Criteria (TSC) for specific control wording. CCB.1-POF15 Considers System Resilience CCB.1-POF15 Considers System Resilience CCB.1-POF16 Protects Confidential Information Information Information Information Information Information	CC8.1-POF14	Manages Patch Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Program	CHG-01	program.	5	
CCB.1-POF14 Manages Patch Changes CCB.1-POF14 Manages Patch Changes Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Functional Intersects with CCB.1-POF15 Considers System Resilience CCB.1-POF15 Considers System Resilience CCB.1-POF16 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Functional Intersects with CCB.1-POF16 Protects Confidential Information CCB.1-POF16 Protects Confiden	CC8.1-POF14	Manages Patch Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Control	CHG-02		5	
CCB.1-POF14 Manages Patch Changes Considers System Resilience Considers System Resilience Considers System Resilience Considers System Resilience CCB.1-POF15 Considers System Resilience CCB.1-POF16 Considers System Resilience Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Functional Intersects with CCB.1-POF16 CCB.1-POF16	CC8.1-POF14	Manages Patch Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management Program	VPM-01		5	
CCB.+POF15 Considers System Realilence CCB.+POF15 Considers System Realilence CCB.+POF15 Considers System Realilence CCB.+POF16 Protects Confidential Information CCB.+POF16 Pro	CC8.1-POF14	Manages Patch Changes	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Software & Firmware	VPM-05	applications and firmware.	5	
Resilience CCB.1-POF15 Considers System Resilience Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with CCB.1-POF16 Protects Confidential Information CCB.1-POF16 Protects Confidential Information	CC8,1-POF15		Download AICPA's Trust Services Criteria (TSC) for specific control wording	Functional	intersects with	Business Continuity	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan	5	
CCB.1-POF15 Considers System Resilience CCB.1-POF15 Considers System Resilience CCB.1-POF15 Considers System Resilience CCB.1-POF16 Protects Confidential information CCB.1-POF16 Protects Confidential inform			Troop or specific contact warming.		will	(BCMS)				
CC8.+POF15 Considers System Resilience Resil	CC8.1-POF15		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		SEA-01	cybersecurity & data privacy practices in the specification, design, development,	5	
Resilience CCB.+POF16 Protects Confidential information CCB.+POF16 Protects Confidential Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional information intersects with Data Protection CD.+OF16 Protects Confidential Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Data Protection CD.+OF16 Protects Confidential Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional intersects with Data Protection CD.+OF16 Protects Confidential Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Data Protection CD.+OF16 Protects Confidential Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Data Protection CD.+OF16 Protects Confidential Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Data Protection CD.+OF16 Protects Confidential Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Data Protection CD.+OF16 Protects Confidential Download AICPA's Trust Services	CC8.1-POF15		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse	5	
CCB.+POF16 Information Download AICPA's trust Services Criteria (TSC) for specific control wording. Functional intersects with Program CFIL-01 program. CFIL-02 program. S CFIL-03 program. S CFIL-04 program.								Mechanisms exist to facilitate the implementation of a change management	-	
CC8.1-POF16 Protects Confidential Information Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Intersects with	CC8.1-POF16	Information	มายหาเอชน ArCPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Program	CHG-01		5	
CC8.1-POF16 Protects Confidential Information CO8.1-POF16 Protects Confidential CO8.1-POF16 Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Data Protection Underspility & Patch Machanisms exist to facilitate the implementation of data protection controls. 5 Witherability & Patch Machanisms exist to facilitate the implementation and monitoring of vulnerability management Program management Program management controls. 5	CC8.1-POF16		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with		CHG-02.2	production environment before changes are implemented in a production	5	
CC3.1-POF16 Protects Confidential Information Download AICPA's Trust Services Criteria (TSC) for specific control wording. Functional Intersects with Inter	CC8.1-POF16		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Protection	DCH-01		5	
	CC8 1-BOE10	Protects Confidential	Download AICPA's Trust Services Criteria (TSC) for specific control words:	Functional	intersects with		VPM.01			
	500. I-FUF 10	Information		. anconat	rsects With		v.rineU1	managarithit unit uis.		



Secure Controls Framework (SCF) 28 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)
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 operating systems, applications and firmware.	5	
CC8.1-POF17	Protects Personal	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	
	Information Protects Personal				Sensitive / Regulated Data		Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
CC8.1-POF17	Information Protects Personal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection	DCH-01.2	Mechanisms exist to facilitate the implementation and operation of data protection	5	
CC8.1-POF17	Information	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 nnoessed lawfully. fairly and transparently. Mechanisms exist to facilitate the implementation and operation of data protection	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	controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully. fairly and transparently.	10	
CC8.1-POF18	Privacy by Design	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Restrict Collection To	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,	5	
	.,,,				Identified Purpose		including protections against collecting PD from minors without appropriate parental or legal guardian consent. Mechanisms exist to determine and document the legal authority that permits the		
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	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	Brisnou by Donigo	Download AICRA's Trust Saniose Criterio (TSC) for especific control wording	Functional	intersects with	Secure Engineering	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized	5	
CC8.1-POF18	Privacy by Design	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Principles Business Continuity	SEA-UI	cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services. Mechanisms exist to facilitate the implementation of contingency planning controls	•	
CC9.1	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 assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Alternative Security	BCD-07	Mechanisms exist to implement alternative or compensating controls to satisfy security functions when the primary means of implementing the security function is	5	
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Measures Risk Management	RSK-01	unavailable or compromised. Mechanisms exist to facilitate the implementation of strategic, operational and	5	
CC9.1	N/A	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	
CC9.1	N/A	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	
							Mechanisms exist to implement a threat intelligence program that includes a cross-		
CC9.1	N/A	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	
CC9.1	N/A	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	
CC9.1	N/A	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. Mechanisms exist to identify, prioritize and assess suppliers and partners of critical	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 systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
							Mechanisms exist to: (1) Evaluate security risks and threats associated with the services and product		
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	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 systems, system components or	5	
					Tools & Methods		Services. Mechanisms exist to utilize security safeguards to limit harm from potential		
CC9.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Limit Potential Harm Processes To Address	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	
CC9.1	N/A	Downtoad AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Weaknesses or Deficiencies Third-Party Processing,	TPM-03.3	the supply chain Mechanisms exist to restrict the location of information processing/storage based	5	
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.	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	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect	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	Its systems, processes and data. Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	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	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure 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	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity &	5	
					Services Third-Party Deficiency		data privacy controls. Mechanisms exist to address weaknesses or deficiencies in supply chain elements		
CC9.1	N/A	Downtoad AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Remediation	TPM-09	identified during independent or organizational assessments of such elements. Mechanisms exist to control changes to services by suppliers, taking into account	5	
CC9.1	N/A	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 information, systems and processes that are in scope by the third-party.	5	
	Considers Mitigation of				Business Continuity		Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan		
CC9.1-POF1	Risks of Business Disruption	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management System (BCMS)	BCD-01	(COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
CC9.1-POF1	Considers Mitigation of Risks of Business	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Compensating	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
CC9.1-POF1	Disruption	Downtosa AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Countermeasures	HSK-06.2		٥	
CC9.1-POF1	Considers Mitigation of Risks of Business	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Impact Analysis	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	5	
CCS. IFOF I	Disruption	Downtoad AICFA's Trast Services Citiena (190) for specific control wording.	Functional	intersects with	(BIA)	NJK-08		٠	
CC9.1-POF2	Considers the Use of Insurance to Mitigate	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 assets and services (e.g., Continuity of Operations Plan	5	
	Financial Impact Risks Considers the Use of				(BCMS) Compensating		(COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks). Mechanisms exist to identify and implement compensating countermeasures to		
CC9.1-POF2	Insurance to Mitigate Financial Impact Risks Considers the Use of	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Countermeasures	RSK-06.2	reduce risk and exposure to threats.	5	
CC9.1-POF2	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	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 of	10	
GC9.2	with vendors and business partners.	DOWNWAS ALEMA S TRUST SERVICES CITIETIS (ISC) for specific control wording.	runctional	SUDSET OF	Management (SCRM) Plan	H5K-U9	systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	10	
CC9.2	The entity assesses and manages risks associated	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Supply Chain Risk	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	5	
	with vendors and business partners. The entity assesses and				Assessment	56.1	Mechanisms exist to facilitate the implementation of third-party management	ļ -	
CC9.2	manages risks associated with vendors and business	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Third-Party Management	TPM-01	reconstraints exist to racilitate the implementation of third-party management controls.	10	
	partners. The entity assesses and manages risks associated				Third-Party Risk		Mechanisms exist to conduct a risk assessment prior to the acquisition or		
CC9.2	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	outsourcing of technology-related services.	5	
000 0 000	Establishes Requirements	Download ACRA's Trust Sanitary Critical (TOO)	Eurosto	Inter	Supply Chain Risk	Don	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of	-	
CC9.2-POF1	for Vendor and Business Partner Engagements	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management (SCRM) Plan	RSK-09	systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
CC9.2-POF1	Establishes Requirements for Vendor and Business	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 systems, system components and services.	5	
CC9.2-POF1	Partner Engagements Establishes Requirements for 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 Fngagements Establishes Requirements				Supply Chain Risk		Mechanisms exist to:		
CC9.2-POF1	for Vendor and Business Partner Engagements	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management (SCRM)	TPM-03	(1) Evaluate security risks and threats associated with the services and product supply chains: and	5	



Secure Controls Framework (SCF) 29 of 4



Set Theory Relationship Mapping (STRM)

ecure Controls Framework (SCF) 30 of



CC9.2-POF13

ownload AICPA's Trust Services Criteria (TSC) for specific control wording

Secure Controls Framework (SCF)

5

chanisms exist to detect vulnerabilities and configuration errors by routin nerability scanning of systems and applications.

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)
	Privacy Criteria Related to Notice and						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	(optional)	
P1.0	Communication of Objectives Related to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Data Privacy Program	PRI-01	processed lawfully, fairly and transparently.	10	
P1.1	Privacy 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 being collected that includes: (1) Notice of the authority of organizations to collect Personal Data (PD): (2) Whether providing PD is mandatory or optional; (3) The principal purpose or purposes for which the PD is to be used; (4) The intended disclosures 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: (1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role: (2) Ensure that organizational data privacy practices are publicly available through	5	
P1.1	N/A	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 prively 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 criters required by applicable statutory, regulatory and contractual obligations. (4) Define the soope 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) Percideally, 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-POF1	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: 1) Make data prively notice(s) evaluable 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, 3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodicatly, review and update the content of the privacy notice, as necessary.	5	
P1.1-POF1	Communicates 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-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 for 11) Make data proxy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; 22 Ensure that data principy notices are clear and easy-to-understand, expressing relevant information about how Personal Data IPD) is collected, received, processed, stored, transmitted, shared, updated and disposed; 13) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligation; 14) Darine 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. (3) Personal call, review and update the content of the privacy notice, as necessary; and (3) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
P1.1-POF2	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+P0F3	Covers Entities 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 prively 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 obligation. (4) Define the scope of PD processing activities, including the geographic locations and third-arry recipients that process the PD within the scope of the data privacy notice. (3) Periodically, review and update the content of the privacy notice, as necessary; and (3) Periodically, review and update the content of the privacy notice, as necessary; and	5	
P1.1-POF3	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		5	
P1.1-P0F4	Uses Clear Language and Presents a Current Privacy Notice in a Location Easily Found by Data Subjects [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Privacy Notice	PRI-02	(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-POF4	Uses Clear Language and Presents a Current Privacy Notice in a Location Easily	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Purpose Specification	PRI-02.1		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	sharari Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
-								-	



FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF# Secure Controls Framework (SCF) Strength of Relationship Notes (optional) (optional) (optional)
P1.1-POFS	Reviews the Privacy Notice [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording:	Functional	intersects with	Data Privacy Notice	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 relevent information about how Personal Data (PD) is collected, received, processed, stored, transities, shared, updead 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 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.
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	Mechanisms exist to: (1) Essure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPC) or similar role; (2) Essure that organizational data privacy practices are publicly available through organizational websites no document repositionise; (3) Utilize publicly facing email adversess and/or phone lines to enable the public to provide herback and/or error determined adversess and/or phone lines to enable the public to provide herbacks and/or error determined adversess and/or phone lines to enable the public to privacy practices; and (4) Inform data subjects when changes are made to the privacy notice and the nature of such changes in the public to provide herbacks and the nature of such changes are made to the privacy notice and the nature of such changes are made to the privacy notice and the nature of such changes are made to the privacy notice and the nature of such changes are made to the privacy notice and the nature of such changes are made to the privacy notice and the nature of such changes are made to the privacy notice and the nature of such changes are made to the privacy notice and the nature of such changes are made to the privacy notice and the nature of such changes are made to the privacy notice and the nature of such changes are made to the privacy notice and the nature of such changes are made to the privacy notice and the nature of such changes are made to the privacy notice and the nature of such changes are made to the privacy office of the nature
P1.1-POF7	Retains Prior Notices [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Privacy Notice	(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently an encessary. (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 obligations. (4) Enter 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.
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	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 subjects is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; PRI-GO (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.
P2.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Choice & Consent	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 subjects is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; PRI-GO (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.
P2.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Just-In-Time Notice & Updated Consent	Mechanisms east 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, which continues to the configuration of the continues of the
P2.1-POF1	Communicates to Data Subjects [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Choice & Consent	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) Pali in 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 cirtisar required by applicable statutory, regulatory and contractual obligations.
P2.1-POF2	Communicates Consequences of Denying or Withdrawing Consent [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Choice & Consent	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 subjects is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.
P2.1-POF3	Obtains Implicit or Explicit Consent [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Choice & Consent	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) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.
P2.1-POF4	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	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, which or original circimumstances under which an individual gave consent have changed; or
P2.1-POFS	Obtains Explicit Consent for Sensitive Information [C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Choice & Consent	(2) A significant amount of time here assend since an individual state consensed. Mechanisms exist to enable data subjects to subtribute the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subjects to 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.
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	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; PRI-03 (2) A remain for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.
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	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 operants or least quarridan consent.
P3.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Restrict Collection To Identified Purpose	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is solden provided to minimize the collection of Personal Data (PD) to only what is solden provided to the provided including protections against collecting PD from minors without appropriate part of least suurdina consent.
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)	Mechanisms exist to determine and document the legal authority that permits the logical authority that permits the logical authority that permits the permits and/or share personal Data (PD), either generally or in support of a specific business process.
P3.1-POF1	[P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Restrict Collection To Identified Purpose	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, inclinary protections against collecting PD from minors without appropriate assertat or lead auardian consent. Mechanisms exist to minimize the collection of Personal Data (PD) to only what is
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	PRE-chains see seet to minimize the collection of Personal Usia prut) to only what it is added, relevant and intelligent to the purpose identified in the day privacy notice, including protections against collecting PD from minors without appropriate part of the protection against collecting PD from minors without appropriate between the read auxiliary consent.



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)
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	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	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	Primary Sources	PRI-04.2	parental or legal guardian consent. Mechanisms exist to ensure information is directly collected from the data subject, whenever possible.	5	
P3.1-POF4	Informs Data Subjects When Additional Information Is Acquired	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	5	
P3.1-POF4	[P][C] Informs Data Subjects When Additional	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Notice of Correction or	PRI-06.2	parental or legal guardian consent. Mechanisms exist to notify affected data subjects if their Personal Data (PD) has	5	
P3.2	Information Is Acquired [PIIC] N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Processing Change 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;	5	
P3.2		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 27.4 significant amount of time has passed since an individual gave consent.	5	
P3.2-POF1	Informs Data Subjects of Consequences of Failure to Provide Consent [C]	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 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 upser 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	(3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, 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) 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.	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	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes, and (2) Authorizes the use of PD when such information is required for internal testing, training and research purposes, and	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);	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 Bata (PD) (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 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 membor 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	
P4.2-POF1	Retains Personal Information [P][C]	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 Data (PD), including metadata, for an organization-defined time period to fulfill the purposed) 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	
P4.2-POF2	Protects Personal Information [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Security of Personal Data (PD)	PRI-01.6	confidentiality and integrity of the PD.	5	
P4.3 P4.3		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	Sanitization of Personal Data (PD) Information Disposal	DCH-09.	Machanieme eviet to facilitate the conitization of Personal Data (PD)	5	
P4.3		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 purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the	5	
P4.3-POF1	Captures, Identifies, and Flags Requests for Deletion [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Feedback Management	PRI-06.4	organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	
P4.3-POF1	Captures, Identifies, and Flags Requests for Deletion (PIIC)	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data 5 (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the setaterities of their PD.	5	
P4.3-POF2	Disposes of, Destroys, and Redacts Personal Information [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	recovered from these components.	5	
P4.3-POF2	Disposes of, Destroys, and Redacts Personal Information [P][C] Disposes of, Destroys,	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical Media Disposal	DCH-08	Made a land and a land	5	
P4.3-POF2	Disposes of, Destroys, and Redacts Personal Disposes of, Destroys, and Redacts Personal Information [P][C]	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	Information Disposal Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, Gestroy, errases, and/or anonymizes the PD, regardless of the	5	
P4.3-POF3	Destroys Personal Information [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	



Secure Controls Framework (SCF) 34 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)
P4.3-POF3	Destroys Personal Information [P][C] Destroys Personal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Physical Media Disposal	DCH-08	formal procedures.	5	
P4.3-POF3	Destroys Personal Information [P][C] Destroys Personal	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Information Disposal Personal Data (PD)	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information. (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, destroys, erases, and/or amonymizes the PD, regardless of the	5	
P4.3-POF3	Information [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Retention & Disposal	PRI-05	method of storage; and (S) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records). Mechanisms exist to provide authenticated data subjects the ability to:	5	
P5.0	Privacy Criteria Related to Access	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Data Subject Empowerment	PRI-06	To Access their personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the beharif offered to the data subject through garding access; (3) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and dispared; (3) Obtain the subgraphies of their PD; expense of their P	10	
P5.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Updating & Correcting Personal Data (PD)	DCH-22.1	inaccurate or outdated, incorrectly determined regarding impact, or incorrectly deidentified.	5	
P5.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disconnected at the theory of the data exhibits through greating access.	5	
P5.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Feedback Management	PRI-06.4	organization collects, receives, processes, stores, transmits, shares, updates and/or diagnose of their December Date (PD). Mechanisms exist to provide authenticated data subjects the ability to:	5	
P5.1-POF1	Responds to Data Controller Requests [P]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Subject Empowerment	PRI-06	(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the bruthen, 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 specifice on how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD (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 inaccursacies; (6) Request correction to their PD due to inaccursacies; (6) Request reasure of their PD, and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
P5.1-POF2	Authenticates Data Subjects' Identity [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Subject Empowerment	PRI-06	Nechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expanse of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain insansers 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 is additionally the processed, stored and shared; (5) Request correction to their PD due to inaccursacies; (6) Request correction or their PD due to inaccursacies; (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD, and	5	
P5.1-POF3	Permits Data Subjects Access to Their Personal Information [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personn Data (Ppl Vinit is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the hearth offered to the data subject through panning 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 is (3) Obtain the conceip of their PD being collected, received, processed, stored and shared; (3) Request correction to their PD due to inaccuracies; (6) Request correction of their PD due to inaccuracies; (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
P5.1-POF4	Provides Understandable Personal Information Within Reasonable Time Provides Understandable Personal Information	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	User Feedback Management Reject Unauthenticated or Untrustworthy Disclosure	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, transmis, shares, updates and/or Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	5	
P5.1-POF5	Within Reasonable Time Informs Data Subjects If Access Is Denied [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Requests User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to comptaints, 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	disposes of their Personal Data (PD). Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is	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 (PD) processed or a process of the CD) isseminating corrections or amendments of PD to other authorized users of the CD.	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	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		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	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 Personal Data (PD)	PRI-12	Mechanisms exist to develop processes to identify and record the method under which Personal Date (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	(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		5	
P5.2-POF2	Communicates Denial of Access Requests [P][C] Permits Data Subjects to	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	Update or Correct Personal Information [PHC]	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	



Secure Controls Framework (SCF) 35 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)
P5.2-POF3	Permits Data Subjects to Update or Correct Personal Information (PIIC)	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-POF3	Permits Data Subjects to Update or Correct Personal Information	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	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	
P6.0	[P][C] 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.	disposes of their Personal Data (PD). Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	10	
P6.1	Notification N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	5	
P6.1-POF1	Communicates Privacy 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	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	5	
P6.1-POF1	Communicates Privacy Policies to Third Parties [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	
P6.1-POF2	Discloses Personal 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.	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized 1 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]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Limiting Personal Data (PD) Disclosures	PRI-01.7	7 for the sole purpose for which the PD was obtained.	5	
P6.1-POF3	Discloses Personal Information Only to Appropriate Third Parties IPIIC1	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Disclosure of Information	DCH-03.	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
P6.1-POF3	Discloses Personal Information Only to Appropriate Third Parties IPIIC1	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	
P6.1-POF4	Discloses Information to Third Parties for New	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Disclosure of Information	DCH-03.	parties with a need to know.	5	
P6.1-POF4	Discloses Information to 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	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	5	
P6.2	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Accounting of Disclosures	PRI-14.1	(1) The organization; and/or	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	(1) The organization; and/or	10	
P6.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Breach	IRO-04.	(2) Relevant third-parties that their PD was shared with. 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	
P6.3	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	
P6.3	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Sensitive / Regulated Data Spill Response	IRO-12	(3) Regulatory authorities. Mechanisms exist to respond to sensitive /regulated data spills.	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	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by: (1) The organization; and/or	5	
P6.3-POF1	Creates and Retains Record of Detected or Reported Unauthorized	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Accounting of Disclosures	PRI-14.1	Relevant third-oarties that their PD was shared with. Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by: (1) The organization; and/or	10	
P6.4	Disclosures [P1 [C1	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	subset of	Data Privacy Requirements for	PRI-07.1	Relevant third-parties that their PD was shared with. Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities	10	
P6.4-POF1	Evaluates Third-Party Compliance With Privacy	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Contractors & Service Providers Disclosure of Information	DCH-03.	for contractors and service providers. Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized 1 parties with a need to know.	5	
P6.4-POF1	Commitments [PIIC] Evaluates Third-Party Compliance With Privacy	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	Remediates Misuse of Personal Information by a	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Limit Potential Harm	TPM-03.	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	Third Party [PI[C] Remediates Misuse of Personal Information by a	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Break Clauses	TPM-05.	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		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	
P6.4-POF3		Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Privacy Requirements for Contractors & Service	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	Disclosures [P][C] Obtains Commitments to Report Unauthorized	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Providers Third-Party Contract	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data	5	
P6.4-POF3	Disclosures [PIIC] Obtains Commitments to Report Unauthorized	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Requirements Contract Flow-Down	TPM-05.	Its systems, processes and data. Mechanisms exist to ensure cybersecurity & data privacy requirements are included	5	
P6.5	Disclosures [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Requirements Third-Party Incident Response & Recovery	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted	5	
P6.5-POF1	Remediates Misuse of	Download AICPA's Trust Services Criteria (ISC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Capabilities Limit Potential Harm	TPM-03.	Mechanisms exist to utilize security safeguards to limit harm from potential	5	
P6.5-POF1	Third Party [PIIC] Remediates Misuse of	Download AICPA's Trust Services Criteria (TSC) for specific control wording. Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional			TPM-05.	Mechanisms exist to include "break clauses" within contracts for failure to meet		
	Third Party [P][C] Remediates Misuse of			intersects with	Break Clauses Third-Party Deficiency		Mechanisms exist to address weaknesses or deficiencies in supply chain elements	5	
P6.5-POF1	Third Party [P][C] Reports Actual or	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	Remediation Limit Potential Harm	TPM-09	Mechanisms exist to utilize security safeguards to limit harm from potential	5	
P6.5-POF2	Disclosures [PI[C] Reports Actual or Suspected Unauthorized	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Break Clauses	TPM-05.	Mechanisms exist to include "break clauses" within contracts for failure to meet	5	
P6.5-POF2	Disclosures [PIIC] Reports Actual or Suspected Unauthorized	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Deficiency	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements	5	
P6.6	Disclosures [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Remediation Data Breach	IRO-04.	Mechanisms exist to address data breaches, or other incidents involving the	5	
P6.6	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Third-Party Incident Response & Recovery	TPM-11	regulations and contractual obligations. Mechanisms exist to ensure response/recovery planning and testing are conducted	5	
P6.6-POF1	Identifies Reporting	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Capabilities Limit Potential Harm	TPM-03.	Mechanisms exist to utilize security safeguards to limit harm from potential 2 adversaries who identify and target the organization's supply chain.	5	
P6.6-POF1	Requirements [P][C] Identifies Reporting Requirements [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Break Clauses	TPM-05.	Mechanisms exist to include "break clauses" within contracts for failure to meet	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	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	equal	Data Breach	IRO-04.		10	
P6.7	[P][C] N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Breach	IRO-04.	regulations and contractual obligations. Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws,	5	
			I	1		L	regulations and contractual obligations.	l	



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)
P6.7	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	ehared Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, update and/or share	5	
	Controller Requests [P]				Personal Data (PD)		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		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.		
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	organization collects, receives, processes, stores, transmits, shares, updates and/o	5	
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	Data Portability	PRI-06.6	discoses 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 without hindrance.	5	
P6.7-POF2	Identifies Types of Personal Information and Handling Process [PIIC]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Personal Data (PD) Exports	PRI-06.7	Mechanisms exist to export a data subject's available Personal Data (PD) in a readily usable format, upon an authenticated request.	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 Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
							Mechanisms exist to receive and process data controller communications pertaining to:	š	
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	(1) Receiving and responding to data subject requests; (2) Updating/correcting Personal Data (PD); (3) Accounting for disclosures of PD; and (4) Accounting for PD that is stored, processed and/or transmitted on behalf of the	5	
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	data controller 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	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Data Quality Management	PRI-10	Information infecedea. 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-POF1	Ensures Accuracy and Completeness of Personal	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	Information [P][C] 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	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 &	PRI-08	information lifecycle. Mechanisms exist to conduct cybersecurity & data privacy testing, training and monitoring activities	5	
P8.1	Enforcement N/A		Functional	intersects with	Monitoring User Feedback	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	5	
P8.1	N/A Communicates to Data	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Management	PRI-06.4	organization collects, receives, processes, stores, transmits, shares, updates and/o disposes of their Personal Data (PD). Mechanisms exist to maintain a process to efficiently and effectively respond to	5	
P8.1-POF1	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	organization collects, receives, processes, stores, transmits, shares, updates and/o disposes of their Personal Data (PD).	5	
P8.1-POF2	Addresses Inquiries, Complaints, and Disputes [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/o discoses of their Personal Data (PD).	5	
P8.1-POF3	Documents and Communicates Dispute Resolution and Recourse [P][C]	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	User Feedback Management	PRI-06.4	organization collects, receives, processes, stores, transmits, shares, updates and/o disposes of their Personal Data (PD).	5	
P8.1-POF4	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	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 statutory, regulatory and contractual requirements.	5	
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	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 statutory, regulatory and contractual requirements.	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	Mechanisms exist to conduct cybersecurity & data privacy testing, training and monitoring activities	5	
PI1.1	N/A	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	,	
PI1.1	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process Definition	PRM-06	& data privacy that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and	5	
					Devillion		(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.		
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	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). Mechanisms exist to require the developer of the output system expressed or	5	
PI1.1	N/A Identifies Functional and	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 Cvcle (SDLC). Mechanisms exist to identify critical system components and functions by	5	
PI1.1-POF1	Nonfunctional Requirements and Information Specifications	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
Du (Identifies Functional and Nonfunctional	Developed MODAL Transferred and College Transferred	Francis	latera e e	Business Process	pp: -	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: (1) The resulting risk to organizational operations, assets, individuals and other	_	
PI1.1-POF1	Requirements and Information Specifications	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	
	Identifies Functional and						abitained Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of products and/or services across the System Development Life Cycle (SDLC) to:		
PI1.1-POF1	Nonfunctional Requirements and Information Specifications	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Product Management	TDA-01.1	(4) Income of continue the	5	
	Identifies Functional and						(4) Conform with applicable statutory, regulatory and/or contractual obligations. Mechanisms exist to design, develop and produce products and/or services in such		
PI1.1-POF1	Nonfunctional and 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	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	



Secure Controls Framework (SCF) 37 of 40



Set Theory Relationship Mapping (STRM)

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)
PI1.3-POF3	Detects and Corrects	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	(optional) 5	
	Processing or Production				Development Practices Service Delivery		Practices (SSIDP) Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning,		
PI1.3-POF4	Records System Processing Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(Business Process Support)	OPS-03		5	
							standards to achieve the specific goals of the process area. Mechanisms exist to define business processes with consideration for cybersecurity		
					Business Process		& data privacy 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	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 Practices (SSDP)	5	
PI1.3-POF5	B	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Freedown		Service Delivery (Business Process	000.00	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning,	5	
PI1.3-POF5	Processes Inputs	Download AICPA's Trust Services Criteria (ISC) 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 coals of the process area. Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines:		
PI1.3-POF5	Processes Inputs	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process	PRM-06	(1) The resulting risk to organizational operations, assets, individuals and other	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	_	
			Functional		Secure Software	TDA-06	ohtsined	5	
PI1.3-POF5	Processes Inputs	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Development Practices	IDA-06	Practices (SSDP). Mechanisms exist to configure systems to produce event logs that contain sufficient	ь	
							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		
PI1.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection of Event Logs	MON-08	(6) The identity of any user/subject associated with the event. Mechanisms exist to protect event logs and audit tools from unauthorized access,	5	
					Access Control for Output		modification and deletion. Physical security mechanisms exist to restrict access to printers and other system		
PI1.4	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Devices	PES-12.2		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,	5	
PIT.4-POFT	Protects Output	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(business Process Support)	UPS-03	business functions, workforce, and/or customers based on industry-recognized	5	
							standards to achieve the specific enals of the process area. Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines:		
PI1.4-POF1	Protects Output	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Business Process	PRM-06	(1) The resulting risk to organizational operations, assets, individuals and other	5	
FILA-FOFT	Protects Output	Download MCFA's Hast Services Citteria (13C) for specific control wording.	Pulictional	littersects with	Definition	r ni-1-00	organizations; and (2) Information protection needs arising from the defined business processes and	3	
					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		
PI1.4-POF1	Protects Output Distributes Output Only to	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Development Practices	TDA-06	Practions (SSDP) Mechanisms exist to develop applications based on Secure Software Development Practions (SSDP) 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 define supporting business processes and implement	5	
PI1.4-POF2	Distributes Output Only to	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,	5	
	Intended Parties				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 & data privacy that determines:		
PI1.4-POF2	Distributes Output Only to	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	
	intended Parties				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		
PI1.4-POF2	Distributes Output Only to	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	
PI1.4-POF3	Intended Parties Distributes Output	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	
	Completely and Distributes Output				Service Delivery		Mechanisms exist to define supporting business processes and implement		
PI1.4-POF3	Completely and Accurately	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(Business Process Support)	OPS-03		5	
	Accurately				Заррого		business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific coals of the process area. Mechanisms exist to define business processes with consideration for cybersecurity		
	Distributes Output						data privacy 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	(1) Information protection needs arising from the defined business processes and	5	
	. Doublety						(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.		
PI1.4-POF3	Distributes Output Completely and	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Secure Software Development Practices	TDA-06	Ontainer Mechanisms exist to develop applications based on Secure Software Development 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	
	Creates and Maintains				Service Delivery		Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning,		
PI1.4-POF4	Records of System Output Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	(Business Process Support)	OPS-03	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		
	Creates and Maintains	Described MODAL Transferred		total Control	Business Process		& data privacy that determines: (1) The resulting risk to organizational operations, assets, individuals and other	_	
PI1.4-POF4	Records of System Output Activities	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Definition	PRM-06	(2) Information protection needs arising from the defined business processes and	5	
	Creates and Maintains				Secure Software		revises the processes as necessary, until an achievable set of protection needs is obtained.		
PI1.4-POF4	Records of System Output	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Development Practices	TDA-06	Machanisms exist to develop applications based on Secure Software Development Practices (SSDP) 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	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls. Mechanisms exist to retain media and data in accordance with applicable statutory,	5	
PI1.5	N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Media & Data Retention	DCH-18	regulatory and contractual obligations. Mechanisms exist to protect event logs and audit tools from unauthorized access,	5	
PI1.5	N/A N/A	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Protection of Event Logs Secure Software	MON-08 TDA-06	modification and deletion. Mechanisms exist to develop applications based on Secure Software Development	5	
PI1.5 PI1.5-POF1	N/A Protects Stored Items	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	Development Practices Data Protection	DCH-01	Practices (SSDP) Mechanisms exist to facilitate the implementation of data protection controls.	5	
.11.51 5F1		South troop to specific control wording.	. anotoliat	seesa witti		_0.1-01	Mechanisms exist to define supporting business processes and implement	-	
PI1.5-POF1	Protects Stored Items	Download AICPA's Trust Services Criteria (TSC) for specific control wording.	Functional	intersects with	Service Delivery (Business Process	OPS-03		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 & data privacy that determines:		
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		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		
PI1.5-POF1	Protects Stored Items	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	
PI1.5-POF2	Archives and Protects	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	
	System Records						Mechanisms exist to define supporting business processes and implement		
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	OPS-03		5	
					Support)	L	business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	L	



Secure Controls Framework (SCF) 39 of



Secure Controls Framework (SCF) 40 of 40