

**NIST IR 8477-Based Set Theory Relationship Mapping (STRM)**

**Reference Document:** Secure Controls Framework (SCF) version 2026.1  
**STRM Guidance:** <https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/>

**Focal Document:**  
**Focal Document URL:**  
**Published STRM URL:**

**Texas DIR Security Control Standards Catalog (v.2.2)**  
[https://dir.texas.gov/sites/default/files/2025-09/Security%20Control%20Standards%20Catalog\\_v2.2.pdf](https://dir.texas.gov/sites/default/files/2025-09/Security%20Control%20Standards%20Catalog_v2.2.pdf)  
<https://content.securecontrolsframework.com/strm/scf-strm-usa-state-tx-dir-security-control-standards-catalog-2.2.pdf>

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Security Control Framework (SCF) Control Description	Strength of Relationship	Notes
AC	Access Control	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AC-01	Policy and Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
AC-01	Policy and Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
AC-01	Policy and Procedures	See FDE for details.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
AC-02	Account Management	See FDE for details.	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	
AC-02	Account Management	See FDE for details.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
AC-02	Account Management	See FDE for details.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
AC-02	Account Management	See FDE for details.	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	
AC-02(3)	Disable Accounts	See FDE for details.	Functional	Equal	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	10	
AC-03	Access Enforcement	See FDE for details.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
AC-03	Access Enforcement	See FDE for details.	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	
AC-03	Access Enforcement	See FDE for details.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
AC-05	Separation Of Duties	See FDE for details.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
AC-05	Separation Of Duties	See FDE for details.	Functional	Intersects With	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).	5	
AC-05	Separation Of Duties	See FDE for details.	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	
AC-05	Separation Of Duties	See FDE for details.	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	
AC-06	Least Privilege	See FDE for details.	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	
AC-06	Least Privilege	See FDE for details.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
AC-06-SID	Least Privilege	Confidential information shall be accessible only to authorized users. An information file or record containing any confidential information shall be identified, documented, and protected in its entirety. Information resources assigned from one state organization to another or from a state organization to a contractor or other third party, at a minimum, shall be protected in accordance with the conditions imposed by the providing state organization.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	8	
AC-07	Unsuccessful Logon Attempts	See FDE for details.	Functional	Equal	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	10	
AC-07-SID.1	Unsuccessful Logon Attempts	As technology permits, state agencies must designate at least one threshold activated by invalid logon attempts (i.e., item a from the control description, an agency-defined number of invalid logon attempts by a user account within an agency-defined time-period).	Functional	Subset Of	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	10	
AC-07-SID.2	Unsuccessful Logon Attempts	As technology permits, state agencies must define, implement, and enforce at least one automatic action that occurs when an agency-defined threshold for invalid logon attempts has been reached (i.e., item b from the control description).	Functional	Subset Of	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	10	
AC-07-SID.3	Unsuccessful Logon Attempts	In designing and implementing access controls for information systems, state agencies should apply a risk-based approach that considers some or all of the following criteria:	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
AC-07-SID.3.a	Unsuccessful Logon Attempts	Capabilities and features of the system;	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
AC-07-SID.3.b	Unsuccessful Logon Attempts	The level of risk presented by the system;	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
AC-07-SID.3.c	Unsuccessful Logon Attempts	Successful application and enforcement of other security controls, such as multifactor authentication, password entropy, and maturity of other authenticator management practices relevant to the information system;	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
AC-07-SID.3.d	Unsuccessful Logon Attempts	The ability to detect and mitigate the risk of other types of attacks focused on authentication (e.g., "account spraying" attacks in which threat actors attempt to access multiple accounts from the same IP address or set of IP addresses without causing many failed logon attempts against each individual account targeted by the threat actors);	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
AC-07-SID.3.e	Unsuccessful Logon Attempts	Whether the system is accessible from the Internet or other public or broadly accessible network(s);	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
AC-07-SID.3.f	Unsuccessful Logon Attempts	Impacts to the agency's users, operations, and support resources if automatic account lockout controls are abused by threat actors to the detriment of account or system availability; and	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
AC-07-SID.3.g	Unsuccessful Logon Attempts	The application of more rigorous controls commensurate to the value and potential for abuse of a type of account (e.g., applying additional controls, enhancements, or overlays to privileged accounts).	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
AC-08	System Use Notification	See FDE for details.	Functional	Equal	System Use Notification (Logon Banner)	SEA-18	Mechanisms exist to utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to Technology Assets, Applications and/or Services (TAAS).	10	
AC-14	Permitted Actions Without Identification Or Authorization	See FDE for details.	Functional	Equal	Permitted Actions Without Identification or Authorization	IAC-26	Mechanisms exist to identify and document the supporting rationale for specific user actions that can be performed on a system without identification or authentication.	10	
AC-17	Remote Access	See FDE for details.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
AC-18	Wireless Access	See FDE for details.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
AC-18	Wireless Access	See FDE for details.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
AC-18-SID	Wireless Access	State agencies shall establish the requirements and security restrictions for installing or providing access to the state agency's information resources systems. The wireless policy shall address the following topic areas:	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
AC-18-SID.1	Wireless Access	Wireless Local Area Networks. Ensure that Service Set Identifiers (SSID) values are changed from the manufacturer default setting.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
AC-18-SID.2	Wireless Access	Transmitting and Encrypting Information. Types of information that may be transmitted via wireless networks and devices with or without encryption including mission critical information or sensitive personal information. State agencies shall not transmit confidential information via a wireless connection to or from a portable computing device unless secure encryption protocols that meet appropriate protection or certification standards as detailed within this Security Control Standards Catalog, are used to protect the information.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by:(1) Authenticating devices trying to connect; and(2) Encrypting transmitted data.	5	
AC-18-SID.3	Wireless Access	Installation or Use of Wireless Personal Area Networks. Prohibit and periodically monitor any unauthorized installation or use of Wireless Personal Area Networks on state agency IT systems by individuals without the approval of the state agency information resources manager.	Functional	Intersects With	Rogue Wireless Detection	NET-15.5	Mechanisms exist to test for the presence of Wireless Access Points (WAPs) and identify all authorized and unauthorized WAPs within the facilities).	5	
AC-19	Access Control For Mobile Devices	See FDE for details.	Functional	Equal	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	10	
AC-19-SID	Access Control For Mobile Devices	State organizations shall establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, whether owned by the state organization or the employee.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5	
AC-20	Use Of External Systems	See FDE for details.	Functional	Equal	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	10	
AC-20-SID	Use Of External Systems	Each state agency entering into or renewing a contract with a vendor authorized to access, transmit, use, or store data for the agency shall include a provision in the contract requiring the vendor to meet the security controls the agency determines are proportionate with the agency's risk under the contract based on the sensitivity of the agency's data. A state agency must require the vendor to periodically provide evidence to the agency that the vendor meets the security controls required under the contract.	Functional	Intersects With	Adequate Security for Sensitive / Regulated Data in Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive/regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
AC-22	Publicly Accessible Content	See FDE for details.	Functional	Equal	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
AT	Awareness and Training	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AT-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
AT-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
AT-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
AT-02	Literacy Training And Awareness	See FDE for details.	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	
AT-02	Literacy Training And Awareness	See FDE for details.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
AT-02-SID	Literacy Training And Awareness	Security awareness training shall be delivered in accordance with Texas Government Code § 2063.103.	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	
AT-02(2)	Insider Threat	See FDE for details.	Functional	Equal	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	10	
AT-03	Role-Based Training	See FDE for details.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	5	
AT-03-SID	Role-Based Training	Security awareness training shall be delivered in accordance with Texas Government Code § 2063.103.	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	
AT-04	Training Records	See FDE for details.	Functional	Equal	Security, Compliance & Resilience Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including:(1) Initial security, compliance and resilience awareness training;(2) Recurring awareness training; and(3) Technology Assets, Applications and/or Services (TAAS)-specific training.	10	
AU	Accountability, Audit, and Risk Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AU-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
AU-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
AU-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
AU-02	Event Logging	See FDE for details.	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	
AU-02	Event Logging	See FDE for details.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
AU-02-SID	Event Logging	Information resources systems shall provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or affect the release of confidential information. Appropriate audit trails shall be maintained to provide accountability for updates to mission critical information, hardware and software and for all changes to automated security or access rules. Based on the risk assessment, a sufficiently complete history of transactions shall be maintained to permit an audit of the information resources system by logging and tracing the activities of individuals through the system.	Functional	Intersects With	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	5	
AU-03	Content Of Audit Records	See FDE for details.	Functional	Equal	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:(1) Establish what type of event occurred;(2) When (date and time) the event occurred;(3) Where the event occurred;(4) The source of the event;(5) The outcome (success or failure) of the event; and(6) The identity of any users/subject associated with the event.	10	
AU-04	Audit Log Storage Capacity	See FDE for details.	Functional	Equal	Event Log Storage Capacity	MON-04	Mechanisms exist to allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded.	10	
AU-05	Response To Audit Logging Process Failures	See FDE for details.	Functional	Equal	Response To Event Log Processing Failures	MON-05	Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption.	10	
AU-06	Audit Record Review, Analysis, And Reporting	See FDE for details.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
AU-06	Audit Record Review, Analysis, And Reporting	See FDE for details.	Functional	Intersects With	Audit Level Adjustments	MON-02.6	Mechanisms exist to adjust the level of audit review, analysis and reporting based on evolving threat information from law enforcement, industry associations or other credible sources of threat intelligence.	5	
AU-08	Time Stamps	See FDE for details.	Functional	Intersects With	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5	
AU-08	Time Stamps	See FDE for details.	Functional	Intersects With	Time Stamps	MON-07	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs.	5	
AU-09	Protection Of Audit Information	See FDE for details.	Functional	Equal	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	10	
AU-11	Audit Record Retention	See FDE for details.	Functional	Equal	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	10	
AU-12	Audit Record Generation	See FDE for details.	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	
CA	Assessment, Authorization, and Monitoring	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CA-01	Policies And Procedures	See FDE for details.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
CA-01	Policies And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
CA-01	Policies And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
CA-02	Control Assessments	See FDE for details.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
CA-02	Control Assessments	See FDE for details.	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 security, compliance and resilience controls.	5	
CA-02	Control Assessments	See FDE for details.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
CA-02	Control Assessments	See FDE for details.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
CA-02	Control Assessments	See FDE for details.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
CA-02-SID	Control Assessments	Control assessments shall be conducted at least biennially.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
CA-03	Information Exchange	See FDE for details.	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection:(1) Interface characteristics;(2) Security, compliance and resilience requirements; and;(3) The nature of the information communicated.	5	
CA-03-SID	Information Exchange	Information resources assigned from or shared between one state agency to another or from or between a state agency to a third-party shall be protected in accordance with the conditions imposed by the providing state agency at a minimum.	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection:(1) Interface characteristics;(2) Security, compliance and resilience requirements; and;(3) The nature of the information communicated.	5	
CA-05	Plan Of Action And Milestones	See FDE for details.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	minimum(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable;(7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the	5	
CA-06	Authorization	See FDE for details.	Functional	Equal	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	10	
CA-06-SID	Authorization	The state organization authorizes the information system for processing before operations or when there is a significant change to the system. A senior organizational official, or their delegate, approves the authorization.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	

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
CA-07	Continuous Monitoring	See FDE for details.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
CA-07(4)	Risk Monitoring	See FDE for details.	Functional	Equal	Risk Monitoring	RSK-11	Mechanisms exist to ensure risk monitoring as an integral part of the continuous monitoring strategy that includes monitoring the effectiveness of security, compliance and resilience controls, compliance and change management.	10	
CA-08	Penetration Testing	See FDE for details.	Functional	Equal	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	10	
CA-08-SID	Penetration Testing	Section 2063.405(a)(2), Government Code, requires each state agency implementing an internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information to subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test. Agencies shall perform, or have performed, an external network penetration test every two years at minimum.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
CA-09	Internal System Connections	See FDE for details.	Functional	Equal	Internal System Connections	NET-05.2	Mechanisms exist to control internal system connections through authorizing internal connections of systems and documenting, for each internal connection, the interface characteristics, security requirements and the nature of the information communicated.	10	
CM	Configuration Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CM-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
CM-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
CM-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
CM-02	Baseline Configuration	See FDE for details.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations:(1) At least annually;(2) When required due to so; or(3) As part of system component installations and upgrades.	5	
CM-02	Baseline Configuration	See FDE for details.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
CM-03	Configuration Change Control	See FDE for details.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
CM-03	Configuration Change Control	See FDE for details.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
CM-03-SID	Configuration Change Control	All security-related information resources changes shall be approved by the information owner (or designee) through a change control process.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
CM-04	Impact Analyses	See FDE for details.	Functional	Equal	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	10	
CM-05	Access Restrictions For Change	See FDE for details.	Functional	Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to Technology Assets, Applications and/or Services (TAAS).	5	
CM-05	Access Restrictions For Change	See FDE for details.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
CM-06	Configuration Settings	See FDE for details.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
CM-06	Configuration Settings	See FDE for details.	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	5	
CM-07	Least Functionality	See FDE for details.	Functional	Equal	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.	10	
CM-08	System Component Inventory	See FDE for details.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:(1) Accurately reflects the current TAASD in use;(2) Identifies authorized software products, including business justification details;(3) Is at the level of granularity deemed necessary for tracking and reporting;(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and(5) Is available for review and audit by designated organizational personnel.	5	
CM-08	System Component Inventory	See FDE for details.	Functional	Intersects With	Component Duplication Avoidance	AST-02.3	Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.	5	
CM-10	Software Usage Restrictions	See FDE for details.	Functional	Equal	Software Usage Restrictions	CFG-04	Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.	10	
CM-11	User-Installed Software	See FDE for details.	Functional	Intersects With	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	
CM-11	User-Installed Software	See FDE for details.	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	
CP	Contingency Planning	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CP-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
CP-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
CP-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
CP-02	Contingency Plan	See FDE for details.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
CP-02	Contingency Plan	See FDE for details.	Functional	Intersects With	Ongoing Contingency Planning	BCD-06	decommissioned business practices, including third-party services;(3) Technologies (e.g., new, altered or decommissioned technologies);(4) Data (e.g., changes to data flows and/or data repositories);(5) Facilities (e.g., new,	5	
CP-02-SID	Contingency Plan	State agencies shall maintain written Continuity of Operations Plans in compliance with Section 412.054, Labor Code that address information resources so that the effects of a disaster will be minimized and the state agency will be able either to maintain or quickly resume mission-critical functions.	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	5	
CP-03	Contingency Training	See FDE for details.	Functional	Equal	Contingency Training	BCD-03	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	10	
CP-04	Contingency Plan Testing	See FDE for details.	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	
CP-04	Contingency Plan Testing	See FDE for details.	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	
CP-04-SID	Contingency Plan Testing	Each state organization's written disaster recovery plan will include provisions for annual testing.	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	
CP-06	Alternate Storage Site	See FDE for details.	Functional	Equal	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.	10	
CP-06-SID	Alternate Storage Site	Mission critical information shall be backed up on a scheduled basis consistent with agency recovery point objectives and stored in a manner logically and physically segmented from the production environment accessible only to authorized individuals.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
CP-07	Alternate Processing Site	See FDE for details.	Functional	Equal	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	
CP-08	Telecommunications Services	See FDE for details.	Functional	Intersects With	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.	5	
CP-09	System Backup	See FDE for details.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
CP-09(2)	Test Restoration Using Sampling	See FDE for details.	Functional	Equal	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.	10	
CP-09(3)	Separate Storage for Critical Information	See FDE for details.	Functional	Equal	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.	10	
CP-10	System Recovery And Reconstitution	See FDE for details.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
CP-10	System Recovery And Reconstitution	See FDE for details.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
CP-10	System Recovery And Reconstitution	See FDE for details.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
CP-11	Alternate Communications Protocols	See FDE for details.	Functional	Intersects With	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.	5	
IA	Identification and Authentication	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

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
IA-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRIP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
IA-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Identity & Access Management (IAM)	IA-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
IA-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
IA-02	Identification And Authentication (Organizational Users)	See FDE for details.	Functional	Equal	Identification & Authentication for Organizational Users	IA-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	10	
IA-02-SID	Identification And Authentication (Organizational Users)	Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access.	Functional	Intersects With	Account Management	IA-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
IA-02(1)	Multifactor Authentication To Privileged Accounts	See FDE for details.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IA-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAS); and/ or (3) Non-console access to critical TAA's that store, transmit and/or process sensitive/regulate data.	5	
IA-02(1)	Multifactor Authentication To Privileged Accounts	See FDE for details.	Functional	Intersects With	Local Access to Privileged Accounts	IA-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	
IA-02(1)	Multifactor Authentication To Privileged Accounts	See FDE for details.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and I-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	5	
IA-02(1)	Multifactor Authentication To Privileged Accounts	See FDE for details.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IA-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5	
IA-02(1)	Multifactor Authentication To Privileged Accounts	See FDE for details.	Functional	Intersects With	Network Access to Privileged Accounts	IA-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
IA-02(1)	Multifactor Authentication To Privileged Accounts	See FDE for details.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IA-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	
IA-02(1)	Multifactor Authentication To Privileged Accounts	See FDE for details.	Functional	Intersects With	Hardware Token-Based Authentication	IA-10.7	Automated mechanisms exist to ensure organization-defined token quality requirements are satisfied for hardware token-based authentication.	5	
IA-02(2)	Multifactor Authentication To Non-Privileged Accounts	See FDE for details.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and I-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	5	
IA-02(2)	Multifactor Authentication To Non-Privileged Accounts	See FDE for details.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IA-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	
IA-02(2)	Multifactor Authentication To Non-Privileged Accounts	See FDE for details.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IA-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5	
IA-02(2)	Multifactor Authentication To Non-Privileged Accounts	See FDE for details.	Functional	Intersects With	Hardware Token-Based Authentication	IA-10.7	Automated mechanisms exist to ensure organization-defined token quality requirements are satisfied for hardware token-based authentication.	5	
IA-02(2)	Multifactor Authentication To Non-Privileged Accounts	See FDE for details.	Functional	Intersects With	Network Access to Privileged Accounts	IA-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
IA-02(2)	Multifactor Authentication To Non-Privileged Accounts	See FDE for details.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IA-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAS); and/ or (3) Non-console access to critical TAA's that store, transmit and/or process sensitive/regulate data.	5	
IA-02(2)	Multifactor Authentication To Non-Privileged Accounts	See FDE for details.	Functional	Intersects With	Local Access to Privileged Accounts	IA-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	
IA-04	Identifier Management	See FDE for details.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IA-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	
IA-04	Identifier Management	See FDE for details.	Functional	Intersects With	Identifier Management (User Names)	IA-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAS).	5	
IA-05	Authenticator Management	See FDE for details.	Functional	Intersects With	Authenticator Management	IA-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	
IA-05	Authenticator Management	See FDE for details.	Functional	Intersects With	Default Authenticators	IA-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
IA-05(1)	Password Based Authentication	See FDE for details.	Functional	Intersects With	Automated Support For Password Strength	IA-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5	
IA-05(1)	Password Based Authentication	See FDE for details.	Functional	Intersects With	Password-Based Authentication	IA-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
IA-05(1)	Password Based Authentication	See FDE for details.	Functional	Intersects With	Authenticator Management	IA-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	
IA-06	Authenticator Feedback	See FDE for details.	Functional	Equal	Authenticator Feedback	IA-11	Mechanisms exist to obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	10	
IA-07	Cryptographic Module Authentication	See FDE for details.	Functional	Intersects With	Cryptographic Module Authentication	IA-12	Mechanisms exist to ensure cryptographic modules adhere to applicable statutory, regulatory and contractual requirements for security strength.	5	
IA-07	Cryptographic Module Authentication	See FDE for details.	Functional	Intersects With	Automated Management of Cryptographic Modules Through Cryptographic Module	CRY-02	Automated mechanisms exist to enable systems to authenticate to a cryptographic module.	5	
IA-08	Identification And Authentication (Non-Organizational Users)	See FDE for details.	Functional	Equal	Identification & Authentication for Non-Organizational Users	IA-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	10	
IA-08-SID	Identification And Authentication (Non-Organizational Users)	Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access.	Functional	Intersects With	Account Management	IA-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
IA-11	Re-Authentication	See FDE for details.	Functional	Equal	Re-Authentication	IA-14	Mechanisms exist to force users and devices to re-authenticate according to organization-defined circumstances that necessitate re-authentication.	10	
IR	Incident Response	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
IR-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
IR-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
IR-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5	
IR-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
IR-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRIP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
IR-01-SID	Incident response policies and procedures shall be reviewed and updated at least every two years.	Incident response policies and procedures shall be reviewed and updated at least every two years.	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5	
IR-02	Incident Response Training	See FDE for details.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	
IR-02-SID	Incident Response Training	The state agency shall train personnel in their incident response roles and responsibilities with respect to the information system and provides training at least annually.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	
IR-03	Incident Response Testing	Testing includes, but is not limited to the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt). Incident response testing can include a determination of the effects on organizational operations and assets and individuals due to incident response and the use of qualitative and quantitative data aids in determining the effectiveness of incident response processes. Incident response plans shall be exercised or tested at least annually.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	
IR-04	Incident Handling	See FDE for details.	Functional	Equal	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
IR-05	Incident Monitoring	See FDE for details.	Functional	Equal	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	10	
IR-06	Incident Reporting	See FDE for details.	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	

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
IR-06	Incident Reporting	See FDE for details.	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	5	
IR-06	Incident Reporting	See FDE for details.	Functional	Intersects With	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5	
IR-06-SID	Incident Reporting	Reporting of security incidents and the investigation and restoration of operations following a security incident assessed to involve suspected criminal activity shall comply with 1 Texas Administrative Code § 202.23(b) and 1 Texas Administrative Code § 202.73(b).	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	
IR-07	Incident Response Assistance	See FDE for details.	Functional	Equal	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	10	
IR-08	Incident Response Plan	See FDE for details.	Functional	Equal	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	
IR-08-SID	Incident Response Plan	State agencies shall assess the significance of a security incident based upon the business impact on the affected resources and the current and potential technical effect of the incident, e.g., loss of revenue, productivity, access to services, reputation, unauthorized disclosure of confidential information, or propagation to other networks. Incident response plans shall be reviewed every two years at a minimum.	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	
IR-09	Information Spillage Response	See FDE for details.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive/regulated data spills.	5	
IR-09	Information Spillage Response	See FDE for details.	Functional	Intersects With	Sensitive / Regulated Data Spill Responsible Personnel	IRO-12.1	Mechanisms exist to formally assign personnel or roles with responsibility for responding to sensitive/regulated data spills.	5	
MA	Maintenance	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
MA-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	
MA-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	5	
MA-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	
MA-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRPR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
MA-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
MA-02	Controlled Maintenance	See FDE for details.	Functional	Equal	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	10	
MA-04	Nonlocal Maintenance	See FDE for details.	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5	
MA-04	Nonlocal Maintenance	See FDE for details.	Functional	Intersects With	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	5	
MA-04	Nonlocal Maintenance	See FDE for details.	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	
MA-05	Maintenance Personnel	See FDE for details.	Functional	Equal	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	10	
MP	Media Protection	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
MP-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRPR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
MP-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
MP-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
MP-02	Media Access	See FDE for details.	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
MP-02	Media Access	See FDE for details.	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	5	
MP-06	Media Sanitization	See FDE for details.	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	
MP-06	Media Sanitization	See FDE for details.	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	
MP-06	Media Sanitization	See FDE for details.	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5	
MP-06(1)	Review, Approve, Track, Document, And Verify	See FDE for details.	Functional	Equal	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	10	
MP-06(1)-SID	Review, Approve, Track, Document, And Verify	State agencies shall keep a record documenting the removal and completion of sanitization of media that stored confidential information with the following information: • date; • description of the item(s) and serial number(s); • inventory number(s); • the process and sanitization tools used to remove the data or method of destruction; and • the name and address of the organization the equipment was transferred to.	Functional	Intersects With	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	5	
MP-07	Media Use	See FDE for details.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
MP-07	Media Use	See FDE for details.	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
MP-07	Media Use	See FDE for details.	Functional	Intersects With	Prohibit Use Without Owner	DCH-10.2	Mechanisms exist to prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	5	
PE	Physical and Environmental Protection	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
PE-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
PE-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
PE-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRPR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
PE-01-SID	Policy And Procedures	The agency shall train designated employees on environmental control procedures, monitoring, and equipment in case of emergencies or equipment problems.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	5	
PE-02	Physical Access Authorizations	See FDE for details.	Functional	Equal	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	
PE-03	Physical Access Control	See FDE for details.	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	
PE-06	Monitoring Physical Access	See FDE for details.	Functional	Equal	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	10	
PE-08	Visitor Access Records	See FDE for details.	Functional	Equal	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	10	
PE-12	Emergency Lighting	See FDE for details.	Functional	Equal	Emergency Lighting	PES-07.4	Facility security mechanisms exist to utilize and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	10	
PE-13	Fire Protection	See FDE for details.	Functional	Equal	Fire Protection	PES-08	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	10	
PE-14	Environmental Controls	See FDE for details.	Functional	Equal	Temperature & Humidity Controls	PES-09	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	10	
PE-15	Water Damage Protection	See FDE for details.	Functional	Equal	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 properly and known to key personnel.	10	
PE-16	Delivery And Removal	See FDE for details.	Functional	Equal	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	10	
PE-17	Alternate Work Site	See FDE for details.	Functional	Equal	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	10	
PL	Planning	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
PL-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
PL-01	Policy And Procedures	See FDE for details.	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	
PL-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	

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
PL-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
PL-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
PL-01-SID	Policy And Procedures	The state agency information security officer reports annually on state agency information security program in compliance with 1 Texas Administrative Code § 202.23(a) and § 202.73(a).	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5	
PL-02	System Security And Privacy Plans	See FDE for details.	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	
PL-02	System Security And Privacy Plans	See FDE for details.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to develop, document and maintain the Information Assurance Security Plan (ISP) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPPTF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5	
PL-02	System Security And Privacy Plans	See FDE for details.	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/regulatory data flows.	5	
PL-04	Rules Of Behavior	See FDE for details.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5	
PL-04	Rules Of Behavior	See FDE for details.	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	
PL-04	Rules Of Behavior	See FDE for details.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5	
PL-04-SID	Rules Of Behavior	All authorized users (including, but not limited to, state agency personnel, temporary employees, and employees of independent contractors) of the state agency's information resources shall formally acknowledge that they will comply with the security policies and procedures of the state agency or they shall not be granted access to information resources. The state agency head or their designated representative will determine the method of acknowledgement and how often this acknowledgement must be reexecuted by the user to maintain access to state agency information resources.	Functional	Intersects With	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.	5	
PL-04(1)	Social Media And External Site/Application Usage Restrictions	See FDE for details.	Functional	Equal	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	10	
PL-10	Baseline Selection	See FDE for details.	Functional	Equal	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
PL-10-SID	Baseline Selection	The default baseline for an information system shall be the controls contained in the Security Controls Catalog. The agency head may employ standards for the cost-effective information security of information, information resources, and applications within or under the supervision of that state agency that are more stringent than the standards the department prescribes under this section if the more stringent standards:	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
PL-10-SID.1	Baseline Selection	contain at least the applicable standards issued by the department; and/or	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
PL-10-SID.2	Baseline Selection	are consistent with applicable federal law, policies, and guidelines issued under state rule, industry standards, best practices, or deemed necessary to adequately protect the information held by the state agency.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
PL-11	Baseline Tailoring	See FDE for details.	Functional	Equal	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	10	
PL-11-SID	Baseline Tailoring	The agency head may employ standards for the cost-effective information security of information, information resources, and applications within or under the supervision of that state agency that are more stringent than the standards the department prescribes under this section if the more stringent standards:	Functional	Intersects With	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
PL-11-SID.1	Baseline Tailoring	contain at least the applicable standards issued by the department; and/or	Functional	Intersects With	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
PL-11-SID.2	Baseline Tailoring	are consistent with applicable federal law, policies, and guidelines issued under state rule, industry standards, best practices, or deemed necessary to adequately protect the information held by the state agency.	Functional	Intersects With	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
PM	Program Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
PM-01	Information Security Program Plan	See FDE for details.	Functional	Subset Of	Security, Compliance & Resilience Program (SCR)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
PM-01	Information Security Program Plan	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
PM-01	Information Security Program Plan	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
PM-02	Information Security Program Role	See FDE for details.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCR).	5	
PM-02-SID	Information Security Program Role	The Information Security Officer is charged with the responsibilities enumerated in Section 2063.401, Government Code and 1 Texas Administrative Code § 202.21 and § 202.71.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCR).	5	
PM-03	Information Security And Privacy Resources	See FDE for details.	Functional	Equal	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCR) and document all exceptions to this requirement.	10	
PM-04	Plan Of Action And Milestones Process	See FDE for details.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
PM-04	Plan Of Action And Milestones Process	See FDE for details.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	Minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency.	5	
PM-05	System Inventory	See FDE for details.	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	
PM-05	System Inventory	See FDE for details.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) is available for review and audit by designated organizational personnel.	5	
PM-05-SID	System Inventory	Agencies shall update system inventories at least every two years.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) is available for review and audit by designated organizational personnel.	5	
PM-05(1)	Inventory of Personally Identifiable Information	See FDE for details.	Functional	Intersects With	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD).	5	
PM-05(1)	Inventory of Personally Identifiable Information	See FDE for details.	Functional	Intersects With	Personal Data (PD) Inventory Automation Support	PRI-05.6	Automated mechanisms exist to determine if Personal Data (PD) is maintained in electronic form.	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
PM-06	Measures Of Performance	See FDE for details.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRPR).	5	
PM-06	Measures Of Performance	See FDE for details.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRPR) measures of performance.	5	
PM-07	Enterprise Architecture	See FDE for details.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	
PM-09	Risk Management Strategy	See FDE for details.	Functional	Equal	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
PM-10	Authorization Process	See FDE for details.	Functional	Equal	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
PM-11	Mission and Business Process Definition	See FDE for details.	Functional	Equal	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes; and revises the processes as necessary, until an achievable set of protection needs is obtained.	10	
PM-14	Testing, Training, And Monitoring	See FDE for details.	Functional	Intersects With	Personal Data (PD) Control Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.	5	
PM-14	Testing, Training, And Monitoring	See FDE for details.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
PM-15	Security And Privacy Groups And Associations	See FDE for details.	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	
PM-15	Security And Privacy Groups And Associations	See FDE for details.	Functional	Intersects With	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the security, compliance and resilience communities to:(1) Facilitate ongoing cybersecurity and data protection education and training for organizational personnel;(2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and(3) Share current cybersecurity and/or data protection-related information including threats, vulnerabilities and incidents.	5	
PM-16	Threat Awareness Program	See FDE for details.	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	
PM-22	Personally Identifiable Information Quality Management	See FDE for details.	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	
PM-22	Personally Identifiable Information Quality Management	See FDE for details.	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 throughout the information lifecycle.	5	
PS	Personnel Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
PS-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
PS-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRPR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
PS-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
PS-02	Position Risk Designation	See FDE for details.	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	
PS-02	Position Risk Designation	See FDE for details.	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	
PS-03	Personnel Screening	See FDE for details.	Functional	Equal	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	
PS-04	Personnel Termination	See FDE for details.	Functional	Equal	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	10	
PS-04-SID	Personnel Termination	User access authorization shall be appropriately modified or removed when the user's employment or job responsibilities within the state agency change.	Functional	Subset Of	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions:(1) Onboarding new personnel (e.g., new hires);(2) Transferring personnel into new roles within the organization; and(3) Offboarding personnel (e.g., termination of employment).	10	
PS-05	Personnel Transfer	See FDE for details.	Functional	Equal	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.	10	
PS-05-SID	Personnel Transfer	User access authorization shall be appropriately modified or removed when the user's employment or job responsibilities within the state agency change.	Functional	Subset Of	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions:(1) Onboarding new personnel (e.g., new hires);(2) Transferring personnel into new roles within the organization; and(3) Offboarding personnel (e.g., termination of employment).	10	
PS-06	Access Agreements	See FDE for details.	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, to both employees and third-parties.	5	
PS-06	Access Agreements	See FDE for details.	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	5	
PS-07	External Personnel Security	See FDE for details.	Functional	Equal	Third-Party Personnel	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.	10	
PS-08	Personnel Sanctions	See FDE for details.	Functional	Equal	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	10	
PS-09	Position Descriptions	See FDE for details.	Functional	Equal	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
RA	Risk Assessment	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
RA-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRPR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
RA-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RA-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
RA-02	Security Categorization	See FDE for details.	Functional	Equal	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that:(1) Document the security categorization results (including supporting rationale) in the security plan for systems; and(2) Ensure the security categorization decision is reviewed and approved by the asset owner.	10	
RA-02-SID	Security Categorization	State agencies are responsible for identifying and defining all information classification categories except the Confidential Information category, as defined by 1 Texas Administrative Code Chapter 202, Subchapter A, and establishing the appropriate controls for each.	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	
RA-03	Risk Assessment	See FDE for details.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
RA-03	Risk Assessment	See FDE for details.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
RA-03-SID	Risk Assessment	The state agency shall perform and document risk assessments and make and document risk management decisions in compliance with 1 Texas Administrative Code § 202.25, § 202.27, § 202.75, and § 202.77.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
RA-03(1)	Supply Chain Risk Assessment	See FDE for details.	Functional	Equal	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	10	
RA-05	Vulnerability Monitoring And Scanning	See FDE for details.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
RA-05	Vulnerability Monitoring And Scanning	See FDE for details.	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	
RA-05-SID	Vulnerability Monitoring And Scanning	The state organization scans for vulnerabilities in the information system at least annually or when significant new vulnerabilities potentially affecting the system are identified and reported.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
RA-05(2)	Update Vulnerabilities To Be Scanned	See FDE for details.	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	
RA-05(11)	Public Disclosure Program	See FDE for details.	Functional	Equal	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	10	
RA-07	Risk Response	See FDE for details.	Functional	Equal	Risk Response	RSK-06.1	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related:(1) Assessments;(2) Audits; and/or(3) Incidents.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SA	System and Services Acquisition	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
SA-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
SA-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
SA-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
SA-02	Allocation Of Resources	See FDE for details.	Functional	Equal	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	
SA-03	System Development Life Cycle	See FDE for details.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5	
SA-03	System Development Life Cycle	See FDE for details.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
SA-04	Acquisition Process	See FDE for details.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
SA-04	Acquisition Process	See FDE for details.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
SA-04	Acquisition Process	See FDE for details.	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	
SA-04	Acquisition Process	See FDE for details.	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5	
SA-04-SID	Acquisition Process	Each state agency entering into or renewing a contract with a vendor authorized to access, transmit, use, or store data for the agency shall include a provision in the contract requiring the vendor to meet the security controls the agency determines are proportionate with the agency's risk under the contract based on the sensitivity of the agency's data. The vendor must periodically provide to the agency evidence that the vendor meets the security controls required under the contract.	Functional	Intersects With	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive/regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
SA-05	System Documentation	See FDE for details.	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	
SA-05	System Documentation	See FDE for details.	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5	
SA-08	Security And Privacy Engineering Principles	See FDE for details.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
SA-08	Security And Privacy Engineering Principles	See FDE for details.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
SA-09	External System Services	See FDE for details.	Functional	Equal	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10	
SA-09-SID	External System Services	Information resources assigned from or shared between one state agency to another or from or between a state agency to a contractor or other third party shall be protected in accordance with the conditions imposed by the providing state agency at a minimum.	Functional	Intersects With	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive/regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
SA-10	Developer Configuration Management	See FDE for details.	Functional	Equal	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	10	
SA-11	Developer Testing And Evaluation	See FDE for details.	Functional	Equal	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	10	
SA-22	Unsupported System Components	See FDE for details.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5	
SA-22	Unsupported System Components	See FDE for details.	Functional	Intersects With	Alternate Sources for Continued Support	TDA-17.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported Technology Assets, Applications and/or Services (TAAS).	5	
SC	System and Communications Protection	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
SC-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
SC-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
SC-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
SC-05	Denial Of Service Protection	See FDE for details.	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	
SC-05	Denial Of Service Protection	See FDE for details.	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5	
SC-05	Denial Of Service Protection	See FDE for details.	Functional	Intersects With	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5	
SC-05	Denial Of Service Protection	See FDE for details.	Functional	Intersects With	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5	
SC-07	Boundary Protection	See FDE for details.	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	
SC-08	Transmission Confidentiality And Integrity	See FDE for details.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
SC-08	Transmission Confidentiality And Integrity	See FDE for details.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
SC-08-SID	Transmission Confidentiality And Integrity	Confidential information that is transmitted over a public network (e.g., the internet) must be encrypted with, at minimum a 128-bit encryption algorithm.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
SC-12	Cryptographic Key Establishment And Management	See FDE for details.	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	
SC-13	Cryptographic Protection	See FDE for details.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
SC-13	Cryptographic Protection	See FDE for details.	Functional	Intersects With	Export-Controlled Cryptography	CRY-01.2	Mechanisms exist to address the exporting of cryptographic technologies in compliance with relevant statutory and regulatory requirements.	5	
SC-13	Cryptographic Protection	See FDE for details.	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	

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
SC-13-SID	Cryptographic Protection	Encryption requirements for information storage devices and data transmissions, as well as specific requirements for portable devices, removable media, and encryption key standards and management shall be based on documented state organization risk management decisions. Confidential information that is transmitted over a public network (e.g., the Internet) must be encrypted. Confidential information stored in a public location that is directly accessible without compensating controls in place (e.g., FTP without access control) must be encrypted. Confidential information must be encrypted if copied to, or stored on, a portable computing device, removable media, or a non-state organization owned computing device. The minimum algorithm strength for protecting confidential information is a 128-bit encryption algorithm, subject to state organization risk management decisions justified and documented in accordance with 1 Texas Administrative Code § 202.21(c) and § 202.71(c) and 1 Texas Administrative Code § 202.25 and §202.75.	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	
SC-15	Collaborative Computing Devices And Applications	See FDE for details.	Functional	Intersects With	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions (1) Networked whiteboards; (2) Video teleconference cameras; and(3) Teleconference microphones.	5	
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	See FDE for details.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5	
SC-21	Secure Name/Address Resolution Service (Recursive Or Caching Resolver)	See FDE for details.	Functional	Equal	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	NET-10.2	Mechanisms exist to perform data origin authentication and data integrity verification on the Domain Name Service (DNS) resolution responses received from authoritative sources when requested by client systems.	10	
SC-22	Architecture And Provisioning For Name/Address Resolution Service	See FDE for details.	Functional	Equal	Architecture & Provisioning for Name / Address Resolution Service	NET-10.1	Mechanisms exist to ensure systems that collectively provide Domain Name Service (DNS) resolution service are fault-tolerant and implement internal/external role separation.	10	
SC-39	Process Isolation	See FDE for details.	Functional	Equal	Process Isolation	SEA-04	Mechanisms exist to implement a separate execution domain for each executing process.	10	
SI	System and Information Integrity	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
SI-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
SI-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
SI-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
SI-02	Flaw Remediation	See FDE for details.	Functional	Intersects With	Vulnerability & Patch Management Program (VPM)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
SI-02	Flaw Remediation	See FDE for details.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
SI-02	Flaw Remediation	See FDE for details.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	
SI-03	Malicious Code Protection	See FDE for details.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
SI-03	Malicious Code Protection	See FDE for details.	Functional	Intersects With	Vulnerability & Patch Management Program (VPM)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
SI-03	Malicious Code Protection	See FDE for details.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
SI-03	Malicious Code Protection	See FDE for details.	Functional	Intersects With	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	
SI-03	Malicious Code Protection	See FDE for details.	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	
SI-03	Malicious Code Protection	See FDE for details.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	
SI-03	Malicious Code Protection	See FDE for details.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-04	System Monitoring	See FDE for details.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-04	System Monitoring	See FDE for details.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
SI-04	System Monitoring	See FDE for details.	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	
SI-04	System Monitoring	See FDE for details.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
SI-05	Security Alerts, Advisories, And Directives	See FDE for details.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-05	Security Alerts, Advisories, And Directives	See FDE for details.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
SI-05	Security Alerts, Advisories, And Directives	See FDE for details.	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	
SI-08	Spam Protection	See FDE for details.	Functional	Equal	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	10	
SI-10	Information Input Validation	See FDE for details.	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	
SI-10	Information Input Validation	See FDE for details.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-12	Information Management And Retention	See FDE for details.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
SI-12	Information Management And Retention	See FDE for details.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRU-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, destroy, erase, and/or anonymize 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	
SR	Supply Chain Risk Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SR-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
SR-01	Policy And Procedures	See FDE for details.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
SR-01	Policy And Procedures	See FDE for details.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
SR-02	Supply Chain Risk Management Plan	See FDE for details.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
SR-02	Supply Chain Risk Management Plan	See FDE for details.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to:(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
SR-03	Supply Chain Controls And Processes	See FDE for details.	Functional	Equal	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	10	
SR-05	Acquisition Strategies, Tools, And Methods	See FDE for details.	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 Technology Assets, Applications and/or Services (TAAS).	5	
SR-08	Notification Agreements	See FDE for details.	Functional	Equal	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	10	
SR-12	Component Disposal	See FDE for details.	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	