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

Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **SCF Data Privacy Management Principles (DPMP) (2025)**
Focal Document URL: https://securecontrolsframework.com/free-scf-content/data-privacy-management-principles-dpmp/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-scf-dpmp-2025.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1	Data Privacy by Design	Establish and maintain a comprehensive data privacy program that ensures data privacy considerations are addressed by design in the development of policies, standards, processes, systems, applications, projects and third-party contracts.	Functional	Intersects With	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.		
1	Data Privacy by Design	Establish and maintain a comprehensive data privacy program that ensures data privacy considerations are addressed by design in the development of policies, standards, processes, systems, applications, projects and third-party contracts.	Functional	Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.		
1	Data Privacy by Design	Establish and maintain a comprehensive data privacy program that ensures data privacy considerations are addressed by design in the development of policies, standards, processes, systems, applications, projects and third-party contracts.	Functional	Intersects With	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to: (1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; (2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; (3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(s) regarding data privacy practices; and (4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.		
1	Data Privacy by Design	Establish and maintain a comprehensive data privacy program that ensures data privacy considerations are addressed by design in the development of policies, standards, processes, systems, applications, projects and third-party contracts.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.		- updated in 2026.1 release
1.1	Assigned Responsibilities	Assign accountability through documented roles and responsibilities to qualified data subjects, including key internal and external stakeholders, for maintaining compliance with all applicable data privacy requirements that involves appropriately monitoring and documenting the data privacy program.	Functional	Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.		
1.1	Assigned Responsibilities	Assign accountability through documented roles and responsibilities to qualified data subjects, including key internal and external stakeholders, for maintaining compliance with all applicable data privacy requirements that involves appropriately monitoring and documenting the data privacy program.	Functional	Intersects With	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program.		- updated in 2026.1 release
1.1	Assigned Responsibilities	Assign accountability through documented roles and responsibilities to qualified data subjects, including key internal and external stakeholders, for maintaining compliance with all applicable data privacy requirements that involves appropriately monitoring and documenting the data privacy program.	Functional	Intersects With	Data Protection Officer (DPO)	PRI-01.4	Mechanisms exist to appoint a Data Protection Officer (DPO): (1) Based on professional qualifications; and (2) To be involved in all issues related to how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed.		
1.2	Data Classification	Classify data according to the sensitivity and type of personal data as defined by appropriate statutory, regulatory and contractual contexts.	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.		
1.2	Data Classification	Classify data according to the sensitivity and type of personal data as defined by appropriate statutory, regulatory and contractual contexts.	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).		
1.3	Registering Databases	Register applicable databases containing personal data with the appropriate Data Authority, when required.	Functional	Intersects With	Register As A Data Controller and/or Data Processor	PRI-15	Mechanisms exist to register as a data controller and/or data processor, including registering databases containing Personal Data (PD) with the appropriate Data Authority, when necessary.		
1.4	Resource Planning	Identify and plan for resources needed to operate a data privacy program and include data privacy requirements in solicitations for Technology Assets, Applications and/or Services (TAAS).	Functional	Intersects With	Cybersecurity & Data Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection-related resource planning controls that define a viable plan for achieving cybersecurity and data protection objectives.		
1.5	Inventory of Personal Data	Maintain an inventory of both the type of personal data and specific data element, as well as the Technology Assets, Applications and/or Services (TAAS) that collect, create, use, disseminate, maintain, and/or disclose that personal data.	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).		

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
1.5	Inventory of Personal Data	Maintain an inventory of both the type of personal data and specific data element, as well as the Technology Assets, Applications and/or Services (TAAS) that collect, create, use, disseminate, maintain, and/or disclose that personal data.	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.		
1.6	Data Privacy Training	Provide recurring data privacy awareness and training for all employees and contractors.	Functional	Intersects With	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.		
1.6	Data Privacy Training	Provide recurring data privacy awareness and training for all employees and contractors.	Functional	Intersects With	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.		
1.6	Data Privacy Training	Provide recurring data privacy awareness and training for all employees and contractors.	Functional	Intersects With	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.		
1.6	Data Privacy Training	Provide recurring data privacy awareness and training for all employees and contractors.	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.		
1.6	Data Privacy Training	Provide recurring data privacy awareness and training for all employees and contractors.	Functional	Intersects With	Practical Exercises	SAT-03.1	Mechanisms exist to include practical exercises in cybersecurity and data protection training that reinforce training objectives.		
1.6	Data Privacy Training	Provide recurring data privacy awareness and training for all employees and contractors.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.		
1.6	Data Privacy Training	Provide recurring data privacy awareness and training for all employees and contractors.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.		
1.6	Data Privacy Training	Provide recurring data privacy awareness and training for all employees and contractors.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity and data protection awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.		- updated in 2026.1 release
1.6	Data Privacy Training	Provide recurring data privacy awareness and training for all employees and contractors.	Functional	Intersects With	Cybersecurity & Data Protection Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including basic cybersecurity and data protection awareness training, ongoing awareness training and specific-system training.		
1.7	Personal Data Categories	Define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).		
1.8	Data Subject Communications	Craft disclosures and communications to data subjects so the material is readily accessible and written in a manner that is concise, unambiguous and understandable by a reasonable person.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.		
1.9	Conspicuous Link To Data Privacy Notice	Design websites and mobile applications to include a conspicuous link to the organization's data privacy notice.	Functional	Intersects With	Conspicuous Link To Data Privacy Notice	PRI-17.1	Mechanisms exist to include a conspicuous link to the organization's data privacy notice on all consumer-facing websites and mobile applications.		
1.10	Notice of Financial Incentive	Provide data subjects with a Notice of Financial Incentive that explains the material terms of a financial incentive, price or service difference so the data subject can make an informed decision about whether to participate.	Functional	Intersects With	Notice of Financial Incentive	PRI-17.2	Mechanisms exist to provide data subjects with a Notice of Financial Incentive that explains the material terms of a financial incentive, price or service difference so the data subject can make an informed decision about whether to participate.		
2	Data Subject Participation	Data subjects are directly involved in the decision-making process regarding the fair and lawful processing of the individual's personal data and, to the extent practicable, directly-engaged to receive explicit permission to use their personal data.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.		
2.1	Clear Choices	Provide clear and conspicuous choices that enable an individual, or a person authorized by the individual, to permit or prohibit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of the individual's personal data. This is also referred to as the right to "opt out."	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.		
2.2	Initial Consent	Prior to the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of the individual's personal data, the knowledge and consent of the individual are required.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.		
2.3	Updated Consent	Based on changes to data privacy practices that affect the parameters of an individual's initial consent, updated consent of the individual is required to continue the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of the individual's personal data. This is also referred to as the right to revoke or "opt out" at any time after the initial consent was provided.	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent.		
2.3	Updated Consent	Based on changes to data privacy practices that affect the parameters of an individual's initial consent, updated consent of the individual is required to continue the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of the individual's personal data. This is also referred to as the right to revoke or "opt out" at any time after the initial consent was provided.	Functional	Intersects With	Revoke Consent	PRI-03.4	Mechanisms exist to allow data subjects to revoke consent to collect, receive, process, store, transmit, share and/or update their Personal Data (PD).		
2.4	Equal Service & Price	Implement business processes to protect the right of data subjects to equal service and price, even if they exercise their data privacy rights.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.		
2.4	Equal Service & Price	Implement business processes to protect the right of data subjects to equal service and price, even if they exercise their data privacy rights.	Functional	Intersects With	Product or Service Delivery Restrictions	PRI-03.5	Mechanisms exist to prevent discrimination against a data subject for exercising their legal rights pertaining to modifying or revoking consent, including prohibiting: (1) Refusing products and/or services; (2) Charging different rates for goods and/or services; and (3) Providing different levels of quality.		- updated in 2026.1 release

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
2.5	Prohibit The Sale of Personal Data	Provide a clear and conspicuous link on the organization's Internet-based homepage, titled "Do Not Sell My Personal Data" that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal data.	Functional	Intersects With	Tailored Consent	PRI-03.1	Mechanisms exist to allow data subjects to modify permission to collect, receive, process, store, transmit, share, update and/or dispose selected attributes of their Personal Data (PD).		
2.5	Prohibit The Sale of Personal Data	Provide a clear and conspicuous link on the organization's Internet-based homepage, titled "Do Not Sell My Personal Data" that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal data.	Functional	Intersects With	Prohibition of Selling, Processing and/or Sharing Personal Data (PD)	PRI-03.3	Mechanisms exist to prevent the sale, processing and/or sharing of Personal Data (PD) when; (1) Instructed by the data subject; or (2) The data subject is a minor, where selling and/or sharing PD is legally prohibited.		
2.6	Authorized Agent (Proxy)	Allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	Functional	Intersects With	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.		
2.7	Global Privacy Control (GPC)	Enable automated mechanisms to provide data subjects with functionality to automatically exercise pre-selected opt-out preferences (e.g., opt-out signal).	Functional	Intersects With	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).		
3	Limited Collection & Use	Ensure that the design of data collection and use are consistent with the intended use of the information and the need for new information is balanced against any data privacy risks.	Functional	Intersects With	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.		
3.1	Authority to Collect	Identify the lawful basis given to collect, create, use, disseminate, maintain, and/or disclose an individual's personal data. Document this authority in the organization's publicly-facing data privacy notice.	Functional	Intersects With	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a specific business process.		
3.2	Data Minimization	Take steps to minimize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of the individual's personal data to what is directly relevant and necessary to accomplish a legally authorized purpose.	Functional	Intersects With	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business practices.		
3.3	Internal Use	Restrict the internal use of personal data to only authorized purpose(s) that are consistent with the stated data privacy notice.	Functional	Intersects With	Minimize Sensitive / Regulated Data	DCH-18.1	Mechanisms exist to minimize sensitive/regulated data that is collected, received, processed, stored and/or transmitted throughout the information lifecycle to only those elements necessary to support necessary business processes.		
3.3	Internal Use	Restrict the internal use of personal data to only authorized purpose(s) that are consistent with the stated data privacy notice.	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.		
3.3	Internal Use	Restrict the internal use of personal data to only authorized purpose(s) that are consistent with the stated data privacy notice.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.		
4	Transparency	Provide a transparent notice to the public about data privacy practices through a clear and conspicuous notice on all organizational websites, mobile applications and other digital services regarding the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of the personal data.	Functional	Intersects With	Privacy Act Statements	PRI-01.2	Mechanisms exist to provide additional formal notice to individuals from whom the information is being collected that includes: (1) Notice of the authority of organizations to collect Personal Data (PD); (2) Whether providing PD is mandatory or optional; (3) The principal purpose or purposes for which the PD is to be used; (4) The intended disclosures or routine uses of the information; and (5) The consequences of not providing all or some portion of the information requested.		

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
4	Transparency	Provide a transparent notice to the public about data privacy practices through a clear and conspicuous notice on all organizational websites, mobile applications and other digital services regarding the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of the personal data.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.		
4	Transparency	Provide a transparent notice to the public about data privacy practices through a clear and conspicuous notice on all organizational websites, mobile applications and other digital services regarding the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of the personal data.	Functional	Intersects With	Notification of Disclosure Request To Data Subject	PRI-14.2	Mechanisms exist to notify data subjects of applicable legal requests to disclose Personal Data (PD).		
4.1	Data Privacy Notice & Purpose Specification	Provide notice of the specific purpose(s) for which personal data is collected, created, used, disseminated, maintained, retained and/or disclosed.	Functional	Intersects With	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.		
4.1	Data Privacy Notice & Purpose Specification	Provide notice of the specific purpose(s) for which personal data is collected, created, used, disseminated, maintained, retained and/or disclosed.	Functional	Intersects With	Notification of Disclosure Request To Data Subject	PRI-14.2	Mechanisms exist to notify data subjects of applicable legal requests to disclose Personal Data (PD).		
5	Data Lifecycle Management	Limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of personal data to that which is legally authorized, relevant and deemed "reasonably necessary" for the proper performance of business functions.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.		
5	Data Lifecycle Management	Limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of personal data to that which is legally authorized, relevant and deemed "reasonably necessary" for the proper performance of business functions.	Functional	Intersects With	Automated Data Management Processes	PRI-02.2	Automated mechanisms exist to adjust data that is able to be collected, received, processed, stored, transmitted, shared, updated and/or disposed, based on updated data subject authorization(s).		
5	Data Lifecycle Management	Limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of personal data to that which is legally authorized, relevant and deemed "reasonably necessary" for the proper performance of business functions.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).		
5	Data Lifecycle Management	Limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of personal data to that which is legally authorized, relevant and deemed "reasonably necessary" for the proper performance of business functions.	Functional	Intersects With	Data Tagging	PRI-11	Mechanisms exist to issue data modeling guidelines to support tagging of sensitive/regulated data.		
5.1	Processing Records	Maintain a record of processing activities that documents the organization's necessary records to support its obligations for the processing of sensitive/regulated data.	Functional	Intersects With	Personal Data (PD) Lineage	PRI-09	Mechanisms exist to maintain a process to document the lineage of Personal Data (PD) by recording how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes PD.		
5.2	Data Flow Mapping	Maintain a record of processing activities that documents the flow of personal data that includes: - Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data; - Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data; - The purposes of the storage, transmission and processing; - A description of the categories of data subjects and personal data; - Where possible, the time limits for erasure of the different categories of data; and - Where possible, a description of the cybersecurity & data privacy measures of the data controller.	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.		- updated in 2026.1 release
5.2	Data Flow Mapping	Maintain a record of processing activities that documents the flow of personal data that includes: - Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data; - Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data; - The purposes of the storage, transmission and processing; - A description of the categories of data subjects and personal data; - Where possible, the time limits for erasure of the different categories of data; and - Where possible, a description of the cybersecurity & data privacy measures of the data controller.	Functional	Intersects With	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulated data is stored, transmitted or processed.		- updated in 2026.1 release
5.2	Data Flow Mapping	Maintain a record of processing activities that documents the flow of personal data that includes: - Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data; - Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data; - The purposes of the storage, transmission and processing; - A description of the categories of data subjects and personal data; - Where possible, the time limits for erasure of the different categories of data; and - Where possible, a description of the cybersecurity & data privacy measures of the data controller.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.		
5.2	Data Flow Mapping	Maintain a record of processing activities that documents the flow of personal data that includes: - Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data; - Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data; - The purposes of the storage, transmission and processing; - A description of the categories of data subjects and personal data; - Where possible, the time limits for erasure of the different categories of data; and - Where possible, a description of the cybersecurity & data privacy measures of the data controller.	Functional	Intersects With	Sensitive / Regulated Data Actions	CFG-08.1	Automated mechanisms exist to generate event logs whenever sensitive/regulated data is collected, created, updated, deleted and/or archived.		

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
5.2	Data Flow Mapping	Maintain a record of processing activities that documents the flow of personal data that includes: - Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data; - Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data; - The purposes of the storage, transmission and processing; - A description of the categories of data subjects and personal data; - Where possible, the time limits for erasure of the different categories of data; and - Where possible, a description of the cybersecurity & data privacy measures of the data controller.	Functional	Intersects With	Sensitive / Regulated Media Records	DCH-01.3	Mechanisms exist to ensure media records for sensitive/regulated data contain sufficient information to determine the potential impact in the event of a data loss incident.		
5.2	Data Flow Mapping	Maintain a record of processing activities that documents the flow of personal data that includes: - Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data; - Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data; - The purposes of the storage, transmission and processing; - A description of the categories of data subjects and personal data; - Where possible, the time limits for erasure of the different categories of data; and - Where possible, a description of the cybersecurity & data privacy measures of the data controller.	Functional	Intersects With	Data Tagging	PRI-11	Mechanisms exist to issue data modeling guidelines to support tagging of sensitive/regulated data.		
5.3	Data Custodians	Identify the owners or operators of Technology Assets, Applications and/or Services (TAAS) that process data, or with which data subjects are interacting.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.		
5.3	Data Custodians	Identify the owners or operators of Technology Assets, Applications and/or Services (TAAS) that process data, or with which data subjects are interacting.	Functional	Intersects With	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.		
5.4	Retention of Personal Data	Ensure that all records containing personal data are maintained in accordance with the organization's records retention schedule and comply with applicable statutory, regulatory and contractual obligations.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.		
5.4	Retention of Personal Data	Ensure that all records containing personal data are maintained in accordance with the organization's records retention schedule and comply with applicable statutory, regulatory and contractual obligations.	Functional	Intersects With	Minimize Sensitive / Regulated Data	DCH-18.1	Mechanisms exist to minimize sensitive/regulated data that is collected, received, processed, stored and/or transmitted throughout the information lifecycle to only those elements necessary to support necessary business processes.		
5.5	Secure Destruction of Personal Data	Utilize secure methods to dispose of or destroy both physical and digital media that contains personal data.	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).		
5.5	Secure Destruction of Personal Data	Utilize secure methods to dispose of or destroy both physical and digital media that contains personal data.	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.		
5.6	Geolocation Restrictions	Restrict the location of processing, storage and service locations to comply with the data privacy notice, as well as applicable statutory, regulatory and contractual obligations.	Functional	Intersects With	Information Location	DCH-24	Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.		
5.6	Geolocation Restrictions	Restrict the location of processing, storage and service locations to comply with the data privacy notice, as well as applicable statutory, regulatory and contractual obligations.	Functional	Intersects With	Transfer of Sensitive and/or Regulated Data	DCH-25	Mechanisms exist to restrict and govern the transfer of sensitive and/or regulated data to third-countries or international organizations.		
5.6	Geolocation Restrictions	Restrict the location of processing, storage and service locations to comply with the data privacy notice, as well as applicable statutory, regulatory and contractual obligations.	Functional	Intersects With	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.		
5.6	Geolocation Restrictions	Restrict the location of processing, storage and service locations to comply with the data privacy notice, as well as applicable statutory, regulatory and contractual obligations.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.		
5.7	Data Portability	Provide the functionality to export personal data in a structured, commonly-used and machine-readable format that can be transferred to another controller without hindrance.	Functional	Intersects With	Data Portability	PRI-06.6	Mechanisms exist to format exports of Personal Data (PD) in a structured, machine-readable format that allows data subjects to transfer their PD to another controller without hindrance.		
5.7	Data Portability	Provide the functionality to export personal data in a structured, commonly-used and machine-readable format that can be transferred to another controller without hindrance.	Functional	Intersects With	Personal Data (PD) Exports	PRI-06.7	Mechanisms exist to export a data subject's available Personal Data (PD) in a readily usable format, upon an authenticated request.		
5.8	Record of Disclosures	Develop and maintain an accounting of personal data disclosures that upon request can be made available to the individual whose personal data was disclosed.	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.		
5.8	Record of Disclosures	Develop and maintain an accounting of personal data disclosures that upon request can be made available to the individual whose personal data was disclosed.	Functional	Intersects With	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by: (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.		
5.9	Integrity Protections	Maintain the accuracy and relevance of personal data across the information lifecycle as personal data is collected, created, used, disseminated, maintained, retained and/or disclosed.	Functional	Intersects With	Data Governance	GOV-10	Mechanisms exist to facilitate data governance to oversee the organization's policies, standards and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.		
5.9	Integrity Protections	Maintain the accuracy and relevance of personal data across the information lifecycle as personal data is collected, created, used, disseminated, maintained, retained and/or disclosed.	Functional	Intersects With	Personal Data (PD) Accuracy & Integrity	PRI-05.2	Mechanisms exist to ensure the accuracy and relevance of Personal Data (PD) throughout the information lifecycle by: (1) Keeping PD up-to-date; and (2) Remediating identified inaccuracies, as necessary.		
5.10	De-Identification	Process personal data in such a manner that it is not attributable to a data subject through technical or organizational measures (e.g., anonymization, pseudonymization or data minimization).	Functional	Intersects With	De-Identification (Anonymization)	DCH-23	Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.		
5.10	De-Identification	Process personal data in such a manner that it is not attributable to a data subject through technical or organizational measures (e.g., anonymization, pseudonymization or data minimization).	Functional	Intersects With	Data Masking	PRI-05.3	Mechanisms exist to mask sensitive/regulated data through data anonymization, pseudonymization, redaction or de-identification.		
5.11	Quality Management	Maintain quality assurances throughout the information lifecycle with such accuracy, relevance, timeliness and completeness as is reasonably necessary to ensure fairness to the individual.	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.		
5.11	Quality Management	Maintain quality assurances throughout the information lifecycle with such accuracy, relevance, timeliness and completeness as is reasonably necessary to ensure fairness to the individual.	Functional	Intersects With	Data Quality Automation	PRI-10.1	Automated mechanisms exist to support the evaluation of data quality across the information lifecycle.		

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
5.12	Secure Data Processing	Implement secure data processing practices so that the confidentiality, integrity and pertinent attributes of sensitive/regulated data is maintained throughout the data lifecycle.	Functional	Intersects With	Cybersecurity & Data Protection In Project Management	PRM-04	Mechanisms exist to assess cybersecurity and data protection controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.		
5.12	Secure Data Processing	Implement secure data processing practices so that the confidentiality, integrity and pertinent attributes of sensitive/regulated data is maintained throughout the data lifecycle.	Functional	Intersects With	Cybersecurity & Data Protection Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).		
5.12	Secure Data Processing	Implement secure data processing practices so that the confidentiality, integrity and pertinent attributes of sensitive/regulated data is maintained throughout the data lifecycle.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.		
5.12	Secure Data Processing	Implement secure data processing practices so that the confidentiality, integrity and pertinent attributes of sensitive/regulated data is maintained throughout the data lifecycle.	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.		
5.12	Secure Data Processing	Implement secure data processing practices so that the confidentiality, integrity and pertinent attributes of sensitive/regulated data is maintained throughout the data lifecycle.	Functional	Intersects With	Manage Organizational Knowledge	PRM-08	Mechanisms exist to manage the organizational knowledge of the cybersecurity and data protection staff.		
5.12	Secure Data Processing	Implement secure data processing practices so that the confidentiality, integrity and pertinent attributes of sensitive/regulated data is maintained throughout the data lifecycle.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).		
5.12	Secure Data Processing	Implement secure data processing practices so that the confidentiality, integrity and pertinent attributes of sensitive/regulated data is maintained throughout the data lifecycle.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).		
5.13	Data Lineage	Maintain records of the inputs, entities and associated Technology Assets, Applications and/or Services (TAAS) that influence data of interest, providing a historical record of the data and its origins.	Functional	Intersects With	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical Technology Assets, Applications and/or Services (TAAS), as well as influence inputs, entities and TAAS, providing a historical record of the data and its origins.		
5.13	Data Lineage	Maintain records of the inputs, entities and associated Technology Assets, Applications and/or Services (TAAS) that influence data of interest, providing a historical record of the data and its origins.	Functional	Intersects With	Personal Data (PD) Lineage	PRI-09	Mechanisms exist to maintain a process to document the lineage of Personal Data (PD) by recording how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes PD.		- updated in 2026.1 release
5.14	Updated Use Permissions	Implement data management processes to adjust data that is able to be collected, created, used, disseminated, maintained, retained and/or disclosed, based on updated data subject authorization(s).	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent.		
5.15	Flaw Remediation with Personal Data	Identify and correct flaws related to personal data as it is collected, created, used, disseminated, maintained, retained and/or disclosed.	Functional	Intersects With	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.		
5.15	Flaw Remediation with Personal Data	Identify and correct flaws related to personal data as it is collected, created, used, disseminated, maintained, retained and/or disclosed.	Functional	Intersects With	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.		- updated in 2026.1 release
5.15	Flaw Remediation with Personal Data	Identify and correct flaws related to personal data as it is collected, created, used, disseminated, maintained, retained and/or disclosed.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.		- updated in 2026.1 release
5.15	Flaw Remediation with Personal Data	Identify and correct flaws related to personal data as it is collected, created, used, disseminated, maintained, retained and/or disclosed.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.		- updated in 2026.1 release
5.15	Flaw Remediation with Personal Data	Identify and correct flaws related to personal data as it is collected, created, used, disseminated, maintained, retained and/or disclosed.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.		- updated in 2026.1 release
5.15	Flaw Remediation with Personal Data	Identify and correct flaws related to personal data as it is collected, created, used, disseminated, maintained, retained and/or disclosed.	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.		- updated in 2026.1 release
5.15	Flaw Remediation with Personal Data	Identify and correct flaws related to personal data as it is collected, created, used, disseminated, maintained, retained and/or disclosed.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.		- updated in 2026.1 release
5.15	Flaw Remediation with Personal Data	Identify and correct flaws related to personal data as it is collected, created, used, disseminated, maintained, retained and/or disclosed.	Functional	Intersects With	Flaw Remediation with Personal Data (PD)	VPM-04.2	Mechanisms exist to identify and correct flaws related to the collection, usage, processing or dissemination of Personal Data (PD).		
5.15	Flaw Remediation with Personal Data	Identify and correct flaws related to personal data as it is collected, created, used, disseminated, maintained, retained and/or disclosed.	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.		- updated in 2026.1 release
5.16	Analytical Biases	Understand and evaluate data analytic inputs and outputs for potential bias.	Functional	Intersects With	Data Analytics Bias	PRI-10.2	Mechanisms exist to evaluate its analytical processes for potential bias.		
6	Data Subject Rights	Provide data subjects with appropriate access to their personal data.	Functional	Intersects With	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).		- updated in 2026.1 release

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
6	Data Subject Rights	Provide data subjects with appropriate access to their personal data.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.		
6	Data Subject Rights	Provide data subjects with appropriate access to their personal data.	Functional	Intersects With	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.		
6.1	Inquiry Management	Maintain a capability to receive and respond to data privacy-related requests, complaints, concerns or questions from data subjects.	Functional	Intersects With	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.		
6.1	Inquiry Management	Maintain a capability to receive and respond to data privacy-related requests, complaints, concerns or questions from data subjects.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.		
6.1	Inquiry Management	Maintain a capability to receive and respond to data privacy-related requests, complaints, concerns or questions from data subjects.	Functional	Intersects With	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).		- updated in 2026.1 release
6.1	Inquiry Management	Maintain a capability to receive and respond to data privacy-related requests, complaints, concerns or questions from data subjects.	Functional	Intersects With	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.		
6.2	Updating Personal Data	Provide data subjects with appropriate opportunity to correct or amend their personal data.	Functional	Intersects With	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.		
6.2	Updating Personal Data	Provide data subjects with appropriate opportunity to correct or amend their personal data.	Functional	Intersects With	Updating Personal Data (PD)	PRI-12	Mechanisms exist to develop processes to identify and record the method under which Personal Data (PD) is updated and the frequency that such updates occur.		
6.3	Redress	Provide data subjects with appropriate opportunity to challenge the organization's compliance with its data privacy principles.	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.		
6.4	Notice of Correction or Amendment	Notify affected data subjects and applicable third-parties when personal data is corrected or amended.	Functional	Intersects With	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected, amended or deleted.		
6.4	Notice of Correction or Amendment	Notify affected data subjects and applicable third-parties when personal data is corrected or amended.	Functional	Intersects With	Obligation To Inform Third-Parties	PRI-07.3	Mechanisms exist to inform applicable third-parties of any modification, deletion or other change that affects shared Personal Data (PD).		
6.5	Appeal	Provide data subjects with appropriate opportunity to appeal an adverse decision to have incorrect personal data amended.	Functional	Intersects With	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.		
6.6	Right to Erasure	Provide data subjects with appropriate opportunity to request the deletion of personal data where it is used, disseminated, maintained, retained and/or disclosed, including where the personal data is stored or processed by third-parties.	Functional	Intersects With	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.		
7	Cybersecurity by Design	Establish administrative, technical and physical safeguards to protect sensitive/regulated data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, Secure Controls Framework (SCF), etc.).	Functional	Intersects With	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application and/or Service (TAAS) under their 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
7	Cybersecurity by Design	Establish administrative, technical and physical safeguards to protect sensitive/regulated data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, Secure Controls Framework (SCF), etc.).	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control.		
7	Cybersecurity by Design	Establish administrative, technical and physical safeguards to protect sensitive/regulated data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, Secure Controls Framework (SCF), etc.).	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control.		
7	Cybersecurity by Design	Establish administrative, technical and physical safeguards to protect sensitive/regulated data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, Secure Controls Framework (SCF), etc.).	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control are implemented correctly and are operating as intended.		
7	Cybersecurity by Design	Establish administrative, technical and physical safeguards to protect sensitive/regulated data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, Secure Controls Framework (SCF), etc.).	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.		
7	Cybersecurity by Design	Establish administrative, technical and physical safeguards to protect sensitive/regulated data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, Secure Controls Framework (SCF), etc.).	Functional	Intersects With	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications and/or Services (TAAS) under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity and data protection controls are operating as intended.		
7	Cybersecurity by Design	Establish administrative, technical and physical safeguards to protect sensitive/regulated data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, Secure Controls Framework (SCF), etc.).	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.		
7	Cybersecurity by Design	Establish administrative, technical and physical safeguards to protect sensitive/regulated data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, Secure Controls Framework (SCF), etc.).	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.		
7	Cybersecurity by Design	Establish administrative, technical and physical safeguards to protect sensitive/regulated data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, Secure Controls Framework (SCF), etc.).	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.		
7	Cybersecurity by Design	Establish administrative, technical and physical safeguards to protect sensitive/regulated data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, Secure Controls Framework (SCF), etc.).	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.		
7	Cybersecurity by Design	Establish administrative, technical and physical safeguards to protect sensitive/regulated data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, Secure Controls Framework (SCF), etc.).	Functional	Intersects With	Centralized Management of Cybersecurity & Data Protection Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity and data protection controls and related processes.		
7	Cybersecurity by Design	Establish administrative, technical and physical safeguards to protect sensitive/regulated data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, Secure Controls Framework (SCF), etc.).	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.		
7	Cybersecurity by Design	Establish administrative, technical and physical safeguards to protect sensitive/regulated data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, Secure Controls Framework (SCF), etc.).	Functional	Intersects With	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity and data protection personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.		
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application and/or Service (TAAS) under their control.		
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control.		
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control.		
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control are implemented correctly and are operating as intended.		
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.		
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications and/or Services (TAAS) under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity and data protection controls are operating as intended.		
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.		
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.		- updated in 2026.1 release

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
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	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.		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.		
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).		
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity and data protection principles that addresses risk to organizational operations, assets, individuals and other organizations.		
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Pre-Established Secure Configurations	TDA-02.4	Mechanisms exist to ensure vendors / manufacturers: (1) Deliver the Technology Asset, Application and/or Service (TAAS) with a pre-established, secure configuration implemented; and (2) Use the pre-established, secure configuration as the default for any subsequent TAAS reinstallation or upgrade.		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Insecure Ports, Protocols & Services	TDA-02.6	Mechanisms exist to mitigate the risk associated with the use of insecure ports, protocols and services necessary to operate technology solutions.		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Cybersecurity & Data Privacy Representatives For Product Changes	TDA-02.7	Mechanisms exist to include appropriate cybersecurity and data privacy representatives in the product feature and/or functionality change control review process.		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Minimizing Attack Surfaces	TDA-02.8	Mechanisms exist to minimize the attack surface of Technology Assets, Applications and/or Services (TAAS) by reasonably mitigating known exploitable vulnerabilities.		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Ongoing Product Security Support	TDA-02.9	Mechanisms exist to deliver security updates to Technology Assets, Applications and/or Services (TAAS), where applicable, through: (1) Automatic updates; and (2) Notification of available updates to affected users.		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Product Testing & Reviews	TDA-02.10	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for an appropriate level of security and resiliency based on applicable risks and threats.		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Disclosure of Vulnerabilities	TDA-02.11	Mechanisms exist to disclose information about vulnerabilities to relevant stakeholders, including: (1) A description of the vulnerability(ies); (2) Affected product(s) and/or service(s); (3) Potential impact of the vulnerability(ies); (4) Severity of the vulnerability(ies); and (5) Guidance to remediate the vulnerability(ies).		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Software Design Review	TDA-06.5	Mechanisms exist to have an independent review of the software design to confirm that all cybersecurity and data protection requirements are met and that any identified risks are satisfactorily addressed.		- updated in 2026.1 release
7.1	Cybersecurity Considerations	Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Technology Assets, Applications and/or Services (TAAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.		- updated in 2026.1 release
7.2	Cryptographic Protections	Ensure personal data is encrypted both at rest and in transit.	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.		
7.2	Cryptographic Protections	Ensure personal data is encrypted both at rest and in transit.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.		
7.2	Cryptographic Protections	Ensure personal data is encrypted both at rest and in transit.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.		
7.3	Physical Protections	Ensure physical security and environmental controls provide appropriate protection for environments where personal data is stored, transmitted and/or processed.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.		
7.3	Physical Protections	Ensure physical security and environmental controls provide appropriate protection for environments where personal data is stored, transmitted and/or processed.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).		- updated in 2026.1 release
7.3	Physical Protections	Ensure physical security and environmental controls provide appropriate protection for environments where personal data is stored, transmitted and/or processed.	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.		- updated in 2026.1 release
7.3	Physical Protections	Ensure physical security and environmental controls provide appropriate protection for environments where personal data is stored, transmitted and/or processed.	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).		- updated in 2026.1 release
7.3	Physical Protections	Ensure physical security and environmental controls provide appropriate protection for environments where personal data is stored, transmitted and/or processed.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.		- updated in 2026.1 release
7.3	Physical Protections	Ensure physical security and environmental controls provide appropriate protection for environments where personal data is stored, transmitted and/or processed.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.		- updated in 2026.1 release
7.3	Physical Protections	Ensure physical security and environmental controls provide appropriate protection for environments where personal data is stored, transmitted and/or processed.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).		- updated in 2026.1 release
7.4	Embedded Technology	Facilitate the secure implementation of embedded technologies so sensors minimize the collection of personal data and alert data subjects to the personal data collected by those sensors.	Functional	Intersects With	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.		
7.4	Embedded Technology	Facilitate the secure implementation of embedded technologies so sensors minimize the collection of personal data and alert data subjects to the personal data collected by those sensors.	Functional	Intersects With	Authorized Use	END-13.1	Mechanisms exist to utilize organization-defined measures so that data or information collected by sensors is only used for authorized purposes.		
7.4	Embedded Technology	Facilitate the secure implementation of embedded technologies so sensors minimize the collection of personal data and alert data subjects to the personal data collected by those sensors.	Functional	Intersects With	Notice of Collection	END-13.2	Mechanisms exist to notify individuals that Personal Data (PD) is collected by sensors.		

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
7.4	Embedded Technology	Facilitate the secure implementation of embedded technologies so sensors minimize the collection of personal data and alert data subjects to the personal data collected by those sensors.	Functional	Intersects With	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.		
7.5	Retire Outdated Systems	Upgrade, replace, or retire any system, application or service for which appropriate protections, commensurate with risk, cannot be effectively implemented.	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.		
7.6	Personnel Security	Implement personnel management practices, covering employees, contractors and other entities, that ensures appropriate vetting and clearance to Technology Assets, Applications and/or Services (TAAS) that contain, store or transmit personal data.	Functional	Intersects With	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.		
7.7	Rules of Behavior	Require employees and contractors to read and agree to abide by the organization's rules of behavior, prior to being granted access to Technology Assets, Applications and/or Services (TAAS) that store, transmit or process personal data, including social media.	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.		
7.7	Rules of Behavior	Require employees and contractors to read and agree to abide by the organization's rules of behavior, prior to being granted access to Technology Assets, Applications and/or Services (TAAS) that store, transmit or process personal data, including social media.	Functional	Intersects With	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.		
7.8	Employee Sanctions	Utilize employee sanctions to hold personnel accountable for complying with the organization's data privacy policies and processes.	Functional	Intersects With	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.		
7.9	Workforce Management	Respond to changing mission requirements and maintain workforce skills in a rapidly-developing technology environment through recruiting and retaining the talent needed to support the organization's mission.	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.		
7.10	Professional Competency	Develop and enforce data privacy competency requirements for staff members involved in the acquisition, management, maintenance and use of information resources, to ensure they have the appropriate knowledge and skill.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.		
7.11	Cybersecurity & Data Privacy Control Validation	Develop and enforce an Information Assurance (IA) capability that provides a mechanism to perform pre-production control testing to ensure applicable cybersecurity & data privacy controls exist and are functioning. Systems, applications and service are prohibited from "going live" without security authorization, following the results of pre-production control testing.	Functional	Intersects With	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.		
7.11	Cybersecurity & Data Privacy Control Validation	Develop and enforce an Information Assurance (IA) capability that provides a mechanism to perform pre-production control testing to ensure applicable cybersecurity & data privacy controls exist and are functioning. Systems, applications and service are prohibited from "going live" without security authorization, following the results of pre-production control testing.	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.		
7.11	Cybersecurity & Data Privacy Control Validation	Develop and enforce an Information Assurance (IA) capability that provides a mechanism to perform pre-production control testing to ensure applicable cybersecurity & data privacy controls exist and are functioning. Systems, applications and service are prohibited from "going live" without security authorization, following the results of pre-production control testing.	Functional	Intersects With	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 cybersecurity and data protection controls, compliance and change management.		
7.11	Cybersecurity & Data Privacy Control Validation	Develop and enforce an Information Assurance (IA) capability that provides a mechanism to perform pre-production control testing to ensure applicable cybersecurity & data privacy controls exist and are functioning. Systems, applications and service are prohibited from "going live" without security authorization, following the results of pre-production control testing.	Functional	Intersects With	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity and data protection personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.		
7.12	Secure Configuration Management	Implement secure configuration management throughout the System Development Life Cycle (SDLC) to ensure Technology Assets, Applications and/or Services (TAAS) are configured according to industry-recognized secure practices.	Functional	Intersects With	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.		
7.12	Secure Configuration Management	Implement secure configuration management throughout the System Development Life Cycle (SDLC) to ensure Technology Assets, Applications and/or Services (TAAS) are configured according to industry-recognized secure practices.	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.		- updated in 2026.1 release
7.12	Secure Configuration Management	Implement secure configuration management throughout the System Development Life Cycle (SDLC) to ensure Technology Assets, Applications and/or Services (TAAS) are configured according to industry-recognized secure practices.	Functional	Intersects With	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity and data protection personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.		
7.13	Situational Awareness	Correlate logs from across the organization with a Security Incident Event Manager (SIEM), or similar automated tool, to maintain situational awareness of events for potential cybersecurity & data privacy incidents.	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.		
7.13	Situational Awareness	Correlate logs from across the organization with a Security Incident Event Manager (SIEM), or similar automated tool, to maintain situational awareness of events for potential cybersecurity & data privacy incidents.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.		
8	Incident Response	Maintain and test incident response plans, capabilities and training for employees and third-party stakeholders on how to report and respond to incidents.	Functional	Intersects With	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.		
8	Incident Response	Maintain and test incident response plans, capabilities and training for employees and third-party stakeholders on how to report and respond to incidents.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.		

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
8	Incident Response	Maintain and test incident response plans, capabilities and training for employees and third-party stakeholders on how to report and respond to incidents.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.		
8	Incident Response	Maintain and test incident response plans, capabilities and training for employees and third-party stakeholders on how to report and respond to incidents.	Functional	Intersects With	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.		
8	Incident Response	Maintain and test incident response plans, capabilities and training for employees and third-party stakeholders on how to report and respond to incidents.	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.		
8	Incident Response	Maintain and test incident response plans, capabilities and training for employees and third-party stakeholders on how to report and respond to incidents.	Functional	Intersects With	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.		
8.1	Coordinated Response	Respond to incidents in a coordinated and structed manner to ensure the appropriate steps are taken to identify and respond to potential incidents.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.		
8.1	Coordinated Response	Respond to incidents in a coordinated and structed manner to ensure the appropriate steps are taken to identify and respond to potential incidents.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.		
8.2	Breach Notification	Report data breaches involving personal data to relevant regulators, law enforcement and affected parties in accordance with applicable statutory, regulatory and contractual obligations for breach notification.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.		
8.2	Breach Notification	Report data breaches involving personal data to relevant regulators, law enforcement and affected parties in accordance with applicable statutory, regulatory and contractual obligations for breach notification.	Functional	Intersects With	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.		
9	Risk Management	Implement a risk management framework to ensure that risks are identified, evaluated and addressed to achieve necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.		
9	Risk Management	Implement a risk management framework to ensure that risks are identified, evaluated and addressed to achieve necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.		- updated in 2026.1 release
9	Risk Management	Implement a risk management framework to ensure that risks are identified, evaluated and addressed to achieve necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	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 cybersecurity and data protection controls, compliance and change management.		
9.1	Evaluate Risks	Utilize appropriate risk analysis methods to evaluate the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of personal data where it is stored, transmitted and/or processed.	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).		
9.1	Evaluate Risks	Utilize appropriate risk analysis methods to evaluate the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of personal data where it is stored, transmitted and/or processed.	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.		- updated in 2026.1 release
9.1	Evaluate Risks	Utilize appropriate risk analysis methods to evaluate the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of personal data where it is stored, transmitted and/or processed.	Functional	Intersects With	Risk Assessment Stakeholder Involvement	RSK-04.4	Mechanisms exist to: (1) Define applicable stakeholders for each risk assessment; (2) Involve identified stakeholders in the risk assessment process; and (3) Provide identified stakeholders with results of the risk assessment, upon completion.		- updated in 2026.1 release
9.2	Assess Supply Chain Risk	Assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS) for data privacy implications.	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.		
9.2	Assess Supply Chain Risk	Assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS) for data privacy implications.	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.		

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
9.2	Assess Supply Chain Risk	Assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS) for data privacy implications.	Functional	Intersects With	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).		
9.3	Risk Awareness	Maintain a current and accurate register of risk (e.g., Plan of Action & Milestones (POA&M), risk register, etc.).	Functional	Intersects With	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.		
9.3	Risk Awareness	Maintain a current and accurate register of risk (e.g., Plan of Action & Milestones (POA&M), risk register, etc.).	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.		
9.3	Risk Awareness	Maintain a current and accurate register of risk (e.g., Plan of Action & Milestones (POA&M), risk register, etc.).	Functional	Intersects With	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 cybersecurity and data protection controls, compliance and change management.		
9.4	Risk Response	Responses to identified risks are appropriately identified, categorized and prioritized.	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity and data protection assessments, incidents and audits to ensure proper remediation has been performed.		
9.5	Data Protection Impact Assessment (DPIA)	Utilize Data Protection Impact Assessments (DPIAs) to effectively identify and reduce data privacy risks to an acceptable level.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.		
10	Third-Party Management	Provide data privacy oversight of third-parties with access to personal data, so that only trusted third-parties are contracted with.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.		
10	Third-Party Management	Provide data privacy oversight of third-parties with access to personal data, so that only trusted third-parties are contracted with.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).		
10	Third-Party Management	Provide data privacy oversight of third-parties with access to personal data, so that only trusted third-parties are contracted with.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.		- updated in 2026.1 release
10	Third-Party Management	Provide data privacy oversight of third-parties with access to personal data, so that only trusted third-parties are contracted with.	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.		- updated in 2026.1 release
10	Third-Party Management	Provide data privacy oversight of third-parties with access to personal data, so that only trusted third-parties are contracted with.	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.		- updated in 2026.1 release
10.1	Supply Chain Protections	Govern the disclosure of personal data to ensure it is only provided to trusted third-parties that can store, process and/or transmit it in a secure manner.	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.		
10.1	Supply Chain Protections	Govern the disclosure of personal data to ensure it is only provided to trusted third-parties that can store, process and/or transmit it in a secure manner.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).		
10.2	Secure Disclosure To Third-Parties	Govern third-party use of personal data to ensure data privacy requirements are enforced when a third-party stores, processes or transmits personal data on behalf of the organization.	Functional	Intersects With	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.		
10.3	Contractual Obligations for Third-Parties	Require terms and conditions in contracts and other agreements to cover the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of personal data.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.		

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
10.3	Contractual Obligations for Third-Parties	Require terms and conditions in contracts and other agreements to cover the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of personal data.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).		
10.3	Contractual Obligations for Third-Parties	Require terms and conditions in contracts and other agreements to cover the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of personal data.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.		
10.4	Third-Party Compliance	Validate that data privacy controls for Technology Assets, Applications and/or Services (TAAS) used or operated by third-parties are effectively-implemented and align with industry-recognized secure practices, as well as comply with applicable statutory, regulatory and contractual obligations.	Functional	Intersects With	Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct cybersecurity and data privacy testing, training and monitoring activities		
10.4	Third-Party Compliance	Validate that data privacy controls for Technology Assets, Applications and/or Services (TAAS) used or operated by third-parties are effectively-implemented and align with industry-recognized secure practices, as well as comply with applicable statutory, regulatory and contractual obligations.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).		
10.4	Third-Party Compliance	Validate that data privacy controls for Technology Assets, Applications and/or Services (TAAS) used or operated by third-parties are effectively-implemented and align with industry-recognized secure practices, as well as comply with applicable statutory, regulatory and contractual obligations.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).		- updated in 2026.1 release
10.4	Third-Party Compliance	Validate that data privacy controls for Technology Assets, Applications and/or Services (TAAS) used or operated by third-parties are effectively-implemented and align with industry-recognized secure practices, as well as comply with applicable statutory, regulatory and contractual obligations.	Functional	Intersects With	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity and data protection control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.		- updated in 2026.1 release
10.4	Third-Party Compliance	Validate that data privacy controls for Technology Assets, Applications and/or Services (TAAS) used or operated by third-parties are effectively-implemented and align with industry-recognized secure practices, as well as comply with applicable statutory, regulatory and contractual obligations.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.		- updated in 2026.1 release
10.4	Third-Party Compliance	Validate that data privacy controls for Technology Assets, Applications and/or Services (TAAS) used or operated by third-parties are effectively-implemented and align with industry-recognized secure practices, as well as comply with applicable statutory, regulatory and contractual obligations.	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.		- updated in 2026.1 release
10.4	Third-Party Compliance	Validate that data privacy controls for Technology Assets, Applications and/or Services (TAAS) used or operated by third-parties are effectively-implemented and align with industry-recognized secure practices, as well as comply with applicable statutory, regulatory and contractual obligations.	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.		- updated in 2026.1 release
11	Business Environment	The organization's mission, objectives, stakeholders and activities are understood and prioritized to provide resourcing and guidance for data privacy roles, responsibilities and risk management decisions.	Functional	Intersects With	Cybersecurity & Data Protection Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity and data protection programs and document all exceptions to this requirement.		
11	Business Environment	The organization's mission, objectives, stakeholders and activities are understood and prioritized to provide resourcing and guidance for data privacy roles, responsibilities and risk management decisions.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.		
11.1	Data Privacy Protections Context	Identify and document the organization's role as a controller and/or processor of sensitive/regulated data, including instances involving more than one party.	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.		
11.1	Data Privacy Protections Context	Identify and document the organization's role as a controller and/or processor of sensitive/regulated data, including instances involving more than one party.	Functional	Intersects With	Joint Processing of Personal Data (PD)	PRI-07.2	Mechanisms exist to clearly define and communicate the organization's role in processing Personal Data (PD) in the data processing ecosystem.		
11.2	Policies, Standards & Procedures	Ensure appropriate policies, standards and procedures exist to operationalize the data privacy program.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.		
11.2	Policies, Standards & Procedures	Ensure appropriate policies, standards and procedures exist to operationalize the data privacy program.	Functional	Intersects With	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to: (1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; (2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; (3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(s) regarding data privacy practices; and (4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.		

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
11.3	Periodic Review	At planned intervals or after significant changes, review policies, standards and procedures to ensure the continuing suitability, adequacy and effectiveness to meet the organization's applicable statutory, regulatory and contractual needs.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.		
11.3	Periodic Review	At planned intervals or after significant changes, review policies, standards and procedures to ensure the continuing suitability, adequacy and effectiveness to meet the organization's applicable statutory, regulatory and contractual needs.	Functional	Intersects With	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements.		
11.4	Oversight	Provide oversight of data privacy controls throughout the lifecycle of Technology Assets, Applications and/or Services (TAAS) to ensure that in a timely manner, senior leaders with the organization are made aware of data privacy-related risks that are not appropriately remediated.	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.		
11.4	Oversight	Provide oversight of data privacy controls throughout the lifecycle of Technology Assets, Applications and/or Services (TAAS) to ensure that in a timely manner, senior leaders with the organization are made aware of data privacy-related risks that are not appropriately remediated.	Functional	Intersects With	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.		
11.5	Metrics & Trends	Provide performance metrics and trend analysis to enable management visibility and coordinate data privacy efforts across the organization.	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program.		
11.5	Metrics & Trends	Provide performance metrics and trend analysis to enable management visibility and coordinate data privacy efforts across the organization.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.		
11.5	Metrics & Trends	Provide performance metrics and trend analysis to enable management visibility and coordinate data privacy efforts across the organization.	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program.		
11.5	Metrics & Trends	Provide performance metrics and trend analysis to enable management visibility and coordinate data privacy efforts across the organization.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.		
11.5	Metrics & Trends	Provide performance metrics and trend analysis to enable management visibility and coordinate data privacy efforts across the organization.	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.		
11.6	Compliance	Oversee the execution of data privacy controls to create appropriate evidence of due diligence and due care, demonstrating compliance with all applicable statutory, regulatory and contractual obligations, including age-based restrictions.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.		
11.6	Compliance	Oversee the execution of data privacy controls to create appropriate evidence of due diligence and due care, demonstrating compliance with all applicable statutory, regulatory and contractual obligations, including age-based restrictions.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.		
11.6	Compliance	Oversee the execution of data privacy controls to create appropriate evidence of due diligence and due care, demonstrating compliance with all applicable statutory, regulatory and contractual obligations, including age-based restrictions.	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.		
11.6	Compliance	Oversee the execution of data privacy controls to create appropriate evidence of due diligence and due care, demonstrating compliance with all applicable statutory, regulatory and contractual obligations, including age-based restrictions.	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-01.3	Mechanisms exist to ensure the organization is able to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.		- updated in 2026.1 release
11.6	Compliance	Oversee the execution of data privacy controls to create appropriate evidence of due diligence and due care, demonstrating compliance with all applicable statutory, regulatory and contractual obligations, including age-based restrictions.	Functional	Intersects With	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.		- updated in 2026.1 release
11.6	Compliance	Oversee the execution of data privacy controls to create appropriate evidence of due diligence and due care, demonstrating compliance with all applicable statutory, regulatory and contractual obligations, including age-based restrictions.	Functional	Intersects With	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.		
11.6	Compliance	Oversee the execution of data privacy controls to create appropriate evidence of due diligence and due care, demonstrating compliance with all applicable statutory, regulatory and contractual obligations, including age-based restrictions.	Functional	Intersects With	Computer Matching Agreements (CMA)	PRI-02.3	Mechanisms exist to publish Computer Matching Agreements (CMA) on the organization's public website(s).		
11.6	Compliance	Oversee the execution of data privacy controls to create appropriate evidence of due diligence and due care, demonstrating compliance with all applicable statutory, regulatory and contractual obligations, including age-based restrictions.	Functional	Intersects With	System of Records Notice (SORN)	PRI-02.4	Mechanisms exist to draft, publish and keep System of Records Notices (SORN) updated in accordance with regulatory guidance.		
11.6	Compliance	Oversee the execution of data privacy controls to create appropriate evidence of due diligence and due care, demonstrating compliance with all applicable statutory, regulatory and contractual obligations, including age-based restrictions.	Functional	Intersects With	System of Records Notice (SORN) Review Process	PRI-02.5	Mechanisms exist to review all routine uses of data published in the System of Records Notices (SORN) to ensure continued accuracy and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.		
11.6	Compliance	Oversee the execution of data privacy controls to create appropriate evidence of due diligence and due care, demonstrating compliance with all applicable statutory, regulatory and contractual obligations, including age-based restrictions.	Functional	Intersects With	Privacy Act Exemptions	PRI-02.6	Mechanisms exist to review all Privacy Act exemptions claimed for the System of Records Notices (SORN) to ensure they remain appropriate and accurate.		
11.7	Critical Business Functions	Ensure Technology Assets, Applications and/or Services (TAAS) that support organizational priorities are assessed so that critical assets are identified and key functional requirements communicated.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.		
11.7	Critical Business Functions	Ensure Technology Assets, Applications and/or Services (TAAS) that support organizational priorities are assessed so that critical assets are identified and key functional requirements communicated.	Functional	Intersects With	Criticality Analysis	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).		
11.7	Critical Business Functions	Ensure Technology Assets, Applications and/or Services (TAAS) that support organizational priorities are assessed so that critical assets are identified and key functional requirements communicated.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.		
11.8	Status Reporting To Governing Body	Provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data privacy program.	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program.		

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: SCF Data Privacy Management Principles (DPMP) (2025)
Focal Document URL: https://securecontrolsframework.com/free-scf-content/data-privacy-management-principles-dpmp/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-scf-dpmp-2025.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	AICPA TSC 2017:2022 (used for SOC 2)	APEC Privacy Framework 2015	GAPP	ISO 27701 2025	ISO 29100 2024	NIST Privacy Framework 1.0	NIST 800-53 R5	NIST 800-53B R5 (privacy)	NIST CSF 2.0	OECD Privacy Principles	US Data Privacy Framework (DPF)	US FIPPS	US HIPAA Administrative Simplification 2013	US - AK PIPA	US - CA CCPA 2025	US - CO Colorado Privacy Act	US - IL BIPA	US - IL IPA	US - IL PIPA	US - NV SB220	US - OR CPA	US - TN Tennessee Information Protection Act	US - TX BC521	US - VA CDPA 2025	US - VT Act 171 of 2018	EMEA EU GDPR	EMEA Saudi Arabia Personal Data Protection Law (PDPL)	APAC Australia Privacy Act	APAC Australian Privacy Principles	APAC India DPDPA 2023	APAC New Zealand Privacy Act of 2020	Americas Canada PIPEDA
1	Data Privacy by Design	Establish and maintain a comprehensive data privacy program that ensures data privacy considerations are addressed by design in the development of policies, standards, processes, systems, applications, projects and third-party contracts.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	5		CC1.1 CC1.1-POF1 CC1.2 CC2.3-POF5		8.2.1	5.1 6.1.3(c) 7.5.1		GV.PO-P1 GV.PO-P6	PM-1		GV GV.RM-01 GV.RM-03 GV.RR-01 GV.SC GV.SC-01 GV.SC-03 GV.SC-09 ID.RA PR PR.IR				164.306(a)(1) 164.306(a)(2) 164.306(a)(3) 164.316(a) 164.530(c)(1)	45.48.530	7123(b)(1)								521.052		2447(a) 2447(a)(1) 2447(a)(1)(A) 2447(a)(1)(B) 2447(a)(1)(C) 2447(a)(1)(D) 2447(a)(2) 2447(b) 2447(c) 2447(c)(1) 2447(c)(1)(A) 2447(c)(1)(A)(i) 2447(c)(1)(A)(ii) 2447(c)(1)(A)(iii) 2447(c)(1)(A)(iv) 2447(c)(1)(A)(v)			APP Part 1 APP Part 11				Principle 7
				Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	5		CC1.3-POF6 CC2.3-POF7 CC8.1-POF17 CC8.1-POF18 P1.0	1 9		4.4 5.1 6.1.1 6.1.1(a) 6.1.1(b) 6.1.3(h) 6.2 6.2(a) 6.2(b) 6.2(c) 6.2(d) 6.2(e) 6.2(f) 6.2(g) 6.3 7.1 7.4 7.5.1 7.5.1(a) 7.5.1(b) 7.5.2 7.5.3	6.10	GV.PO-P1 GV.PO-P5 GV.PO-P6 CT.PO-P2 CM.PO-P1 CM.AW-P2 PR.PO-P9	PM-18 PT-1	PM-18 PT-1	GV.OC-03	8	III.15.a	2	164.502(a) 164.530(a)(1)(i) 164.530(i)(1)		7002(a)	6-1-1305(2) 6-1-1305(7) 6-1-1308(1)(c)(I) 6-1-1308(1)(c)(II) 6-1-1308(6) 6-1-105(1)(nnn)								59.1-578.A.3		12.2 5.1(a) 9.1	11.2	Inferred Expectation	APP 1			Principle 1 Principle 8
				Intersects With	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to:(1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role;(2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories;(3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(s) regarding data privacy practices; and(4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.	5		P1.1 P1.1-POF6		2.1.1 2.2.1 2.2.2 2.2.3 3.1.0 3.1.1 3.1.2 4.1.0 4.1.1 4.2.4 5.1.0 5.1.1 6.1.0 7.1.0 7.1.1 8.1.0 8.1.1 9.1.0 9.1.1 10.1.0 10.1.1	6.2(e) 7.4 7.5.3(a)	6.8	GV.PO-P1 CM.PO-P1 CM.AW-P1	PM-20	PM-20		6		8									7(1)(a)(B)			59.1-581.A.2					APP 1			
				Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	- updated in 2026.1 release		2-1 2-2			6.5 6.8 6.10							2 4			7002(b) 7002(b)(1) 7002(b)(2) 7002(b)(3) 7002(d) 7002(d)(1) 7002(d)(2) 7027(m) 7027(m)(1) 7027(m)(2) 7027(m)(3) 7027(m)(4) 7027(m)(5) 7027(m)(6) 7027(m)(7) 7027(m)(8)									59.1-577.1.B 59.1-577.1.C 59.1-577.1.E 59.1-578.A.4 59.1-578.F.1.d 59.1-578.F.2 59.1-579.A.1 59.1-579.A.2 59.1-579.A.3								
1.1	Assigned Responsibilities	Assign accountability through documented roles and responsibilities to qualified data subjects, including key internal and external stakeholders, for maintaining compliance with all applicable data privacy requirements that involves appropriately monitoring and documenting the data privacy program.	Functional	Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	5		CC1.3-POF6 CC2.3-POF7 CC8.1-POF17 CC8.1-POF18 P1.0	1 9		4.4 5.1 6.1.1 6.1.1(a) 6.1.1(b) 6.1.3(h) 6.2 6.2(a) 6.2(b) 6.2(c) 6.2(d) 6.2(e) 6.2(f) 6.2(g) 6.3 7.1 7.4 7.5.1 7.5.1(a) 7.5.1(b) 7.5.2 7.5.3	6.10	GV.PO-P1 GV.PO-P5 GV.PO-P6 CT.PO-P2 CM.PO-P1 CM.AW-P2 PR.PO-P9	PM-18 PT-1	PM-18 PT-1	GV.OC-03	8	III.15.a	2	164.502(a) 164.530(a)(1)(i) 164.530(i)(1)		7002(a)	6-1-1305(2) 6-1-1305(7) 6-1-1308(1)(c)(I) 6-1-1308(1)(c)(II) 6-1-1308(6) 6-1-105(1)(nnn)								59.1-578.A.3		12.2 5.1(a) 9.1	11.2	Inferred Expectation	APP 1			Principle 1 Principle 8
				Intersects With	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program.	5	- updated in 2026.1 release		9	1.1.0 1.1.2 1.2.1 1.2.2 1.2.8 1.2.9 2.1.0 4.2.3 8.2.1	5.1 5.3	6.10	GV.PO-P5	PM-19	PM-19		8		2	164.530(a)(1)(i)			6-1-1308(1)(c)(I) 6-1-1308(1)(c)(II) 6-1-1308(6)																
				Intersects With	Data Protection Officer (DPO)	PRI-01.4	Mechanisms exist to appoint a Data Protection Officer (DPO):(1) Based on professional qualifications; and(2) To be involved in all issues related to how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed.	5						6.10	GV.PO-P5 CT.PO-P2 CM.PO-P2							164.530(a)(1)(ii)			6-1-1308(1)(c)(I) 6-1-1308(1)(c)(II) 6-1-1308(6)										27.1 27.3 27.4 27.5 35.2 37.1 37.1(a) 37.1(b) 37.1(c) 37.2 37.3 37.4 37.5 37.6 37.7 38.1 38.2 38.3 38.4 38.5 38.6 39.1 39.1(a) 39.1(b) 39.1(c) 39.1(d) 39.1(e) 39.2	30.2			10(2)(a) 10(2)(a)(iv)		Sec 6
1.2	Data Classification	Classify data according to the sensitivity and type of personal data as defined by appropriate statutory, regulatory and contractual contexts.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		C1.1 CC2.1 CC2.1-POF7 CC6.1-POF1								ID.AM-05 PR.DS						7123(c)(4)(A)																	
				Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	5								PT-7 PT-7(1) PT-7(2)	PT-7 PT-7(1) PT-7(2)							7024(j) 7024(l)						5(4)(a) 5(4)(e)			59.1-578.C.4		13.1(e) 14.1(d)			APP 9			
1.3	Registering Databases	Register applicable databases containing personal data with the appropriate Data Authority, when required.	Functional	Intersects With	Register As A Data Controller and/or Data Processor	PRI-15	Mechanisms exist to register as a data controller and/or data processor, including registering databases containing Personal Data (PD) with the appropriate Data Authority, when necessary.	5																										2446(a) 2446(a)(1) 2446(a)(2) 2446(a)(3) 2446(a)(3)(A) 2446(a)(3)(B) 2446(a)(3)(B)(i) 2446(a)(3)(B)(ii) 2446(a)(3)(B)(iii) 2446(a)(3)(C) 2446(a)(3)(D) 2446(a)(3)(E) 2446(a)(3)(F) 2446(a)(3)(G)							
1.4	Resource Planning	Identify and plan for resources needed to operate a data privacy program and include data privacy requirements in solicitations for Technology Assets, Applications and/or Services (TAAS).	Functional	Intersects With	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.	5		CC2.2 CC3.1 CC3.1-POF4 CC3.4 CC5.2			7.1			PL-1	PL-1	GV.RM GV.RR-03																							
1.5	Inventory of Personal Data	Maintain an inventory of both the type of personal data and specific data element, as well as the Technology Assets, Applications and/or Services (TAAS) that collect, create, use, disseminate, maintain, and/or disclose that personal data.	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				7.2.2			ID.IM-P1 ID.IM-P3 ID.IM-P6	PM-5(1)	PM-5(1)	ID.AM-07						7123(c)(4)(A)																	
				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							ID.IM-P1 ID.IM-P3 ID.IM-P6	PM-5(1)	PM-5(1)																								
1.6	Data Privacy Training	Provide recurring data privacy awareness and training for all employees and contractors.	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5		CC1.4 CC1.4-POF3 CC2.2-POF12 CC2.2-POF8					GV.AT-P1 GV.AT-P2 GV.AT-P3 GV.AT-P4	AT-1 PM-13	AT-1	PR.AT				164.308(a)(5)(i)		7123(c)(12)										2447(b)(2)(A) 2447(c)(8)							
				Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5		CC1.4-POF7 CC2.2-POF12 CC2.2-POF8					GV.AT-P1 GV.AT-P2 GV.AT-P3	AT-2	AT-2	PR.AT PR.AT-01				164.308(a)(5)(i) 164.530(b)(2)(i) 164.530(b)(2)(i)(A) 164.530(b)(2)(i)(B) 164.530(b)(2)(i)(C) 164.530(b)(2)(ii)		7100(a) 7123(c)(12) 7123(c)(13)										2447(b)(2)(A) 2447(c)(8)							
				Intersects With	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.	5								AT-2(1) AT-6																									
				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		CC1.4-POF7 CC2.2-POF12 CC2.2-POF13			7.2	6.10	GV.AT-P1 GV.AT-P2 GV.AT-P3	AT-3 AT-3(2)	AT-3	PR.AT PR.AT-01 PR.AT-02			2	164.308(a)(5)(ii)(C) 164.308(a)(5)(ii)(D) 164.530(b)(1)		7100(a) 7123(c)(12) 7123(c)(13)										2447(b)(2)(A) 2447(c)(8)							
				Intersects With	Practical Exercises	SAT-03.1	Mechanisms exist to include practical exercises in security, compliance and resilience training that reinforce training objectives.	5								AT-3(3)																									
				Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5		CC2.2-POF13 CC2.3-POF12						AT-2(4) AT-2(5)						164.308(a)(5)(ii)(B)												2447(c)(4)							
				Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	5		CC2.2-POF9		1.1.1 1.2.10		6.10		AT-3(5)	AT-3(5)				2			7100(a) 7123(c)(12) 7123(c)(13)										2447(c)(8)							
				Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	- updated in 2026.1 release	CC2.2-POF8						AT-2(6)		ID.RA-03				164.308(a)(5)(ii)(A)		7123(c)(12) 7123(c)(13)																	
				Intersects With	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.	5								AT-4	AT-4							7123(c)(12) 7123(c)(13)																	
1.7	Personal Data Categories	Define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	5								PT-7 PT-7(1) PT-7(2)	PT-7 PT-7(1) PT-7(2)							7024(j) 7024(l)						5(4)(a) 5(4)(e)			59.1-578.C.4		13.1(e) 14.1(d)			APP 9			
1.8	Data Subject Communications	Craft disclosures and communications to data subjects so the material is readily accessible and written in a manner that is concise, unambiguous and understandable by a reasonable person.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5		P6.7-POF3														7003(a) 7004(a)(3) 7222(b) 7222(b)(1) 7222(b)(2) 7222(b)(3) 7222(b)(3)(A) 7222(b)(4) 7222(b)(4)(A) 7222(c) 7222(c)(1) 7222(c)(2) 7222(c)(2)(A) 7222(c)(2)(B) 7222(c)(2)(C) 7222(d) 7222(e) 7222(f) 7222(g) 7222(h) 7222(i) 7222(j) 7222(k)									59.1-577.B.2								

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	AICPA TSC 2017+2022 (used for SOC 2)	APEC Privacy Framework 2015	GAPP	ISO 27701 2025	ISO 29100 2024	NIST Privacy Framework 1.0	NIST 800-53 R5	NIST 800-53B R5 (privacy)	WEF CAF 2.0	OECD Privacy Principles	US Data Privacy Framework (DPF)	US FIPPS	US HIPAA Administrative Simplification 2013	US - AK PIPA	US - CA CCPA/CPRA 2025	US - CO Colorado Privacy Act	US - IL BIPA	US - IL IPA	US - IN PIPA	US - NV SB220	US - OR CPA	US - TN Tennessee Information Protection Act	US - TX SCUI	US - VA CDPA 2023	US - VT Act 171 of 2018	EMEA EU GDPR	EMEA Saudi Arabia Personal Data Protection Law (PDPL)	APAC Australia Privacy Act	APAC Australian Privacy Principles	APAC India DPDPA 2023	APAC New Zealand Privacy Act of 2020	Americas Canada PIPEDA
1.9	Conspicuous Link To Data Privacy Notice	Design websites and mobile applications to include a conspicuous link to the organization's data privacy notice.	Functional	Intersects With	Conspicuous Link To Data Privacy Notice	PRI-17.1	Mechanisms exist to include a conspicuous link to the organization's data privacy notice on all consumer-facing websites and mobile applications.	5																	7003(c) 7003(d)															
1.10	Notice of Financial Incentive	Provide data subjects with a Notice of Financial Incentive that explains the material terms of the financial incentive, price or service difference so the data subject can make an informed decision about whether to participate.	Functional	Intersects With	Notice of Financial Incentive	PRI-17.2	Mechanisms exist to provide data subjects with a Notice of Financial Incentive that explains the material terms of the financial incentive, price or service difference so the data subject can make an informed decision about whether to participate.	5																	7010(g) 7080(e)															
2	Data Subject Participation	Data subjects are directly involved in the decision-making process regarding the fair and lawful processing of the individual's personal data and, to the extent practicable, directly engaged to receive explicit permission to use their personal data.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject(s): (1) Receives notice of the organization's data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5		P2.2 P3.1 P3.2 P3.2-POF1 P3.2-POF2 P3.2-POF3 P3.2-POF4 P3.2-POF5 P3.2-POF6 P3.2 P3.2-POF2	2(e) 4(a) 5	1.2.1 1.2.2 1.2.3 3.2.4	6.2	CT.PO-P1 CT.PO-P2	PT-4	PT-4		1 4(a)	6.2.a 6.2.c		164.506(b)(1) 164.508(a)(2) 164.508(a)(3) 164.510(b)(2)(i) 164.510(b)(2)(ii) 164.510(b)(2)(iii) 164.510(b)(3) 164.514(d)(2)(i) 164.514(f)(2)(iv) 164.514(f)(2)(v)		7002(e) 7002(f) 7012(e) 7012(f) 7020(d) 7012(e) 7012(f) 7012(g) 7012(h) 7012(i) 7012(j) 7012(k) 7012(l) 7012(m) 7012(n) 7012(o) 7012(p) 7012(q) 7012(r) 7027(d) 7027(e)	6-1-1306(1) 6-1-1306(1)(a)(I)(A) 6-1-1306(1)(a)(I)(B) 6-1-1306(1)(a)(IV) 6-1-1306(1)(a)(IV) (A) 6-1-1306(1)(a)(IV) (B) 6-1-1306(1)(a)(IV) (C)	15(b)(3)					5(2)(b) 5(2)(c)	47-18-3203(a)(2)(B) 47-18-3203(a)(2)(C) 47-18-3204(a)(B)			59.1-578.A.5 59.1-578.D		21.1 21.2 21.3 21.4 21.5 7.1 7.2 9.2(a)	10.1 15.1 24.1 25.1 25.2 25.3 5.1 5.1	APP Part 1	APP 3	4(1)(a) 4(1)(6)(ii) 6(7) 7(e) 8(3)(a) 8(8)(b)	Sec 6 Sec 7 Principle 3
2.1	Clear Choices	Provide clear and conspicuous choices that enable an individual, or a person authorized by the individual, to permit or prohibit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of the individual's personal data. This is also referred to as the right to "opt out."	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject(s): (1) Receives notice of the organization's data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5		P2.2 P3.1 P3.2 P3.2-POF1 P3.2-POF2 P3.2-POF3 P3.2-POF4 P3.2-POF5 P3.2-POF6 P3.2 P3.2-POF2	2(e) 4(a) 5	1.2.1 1.2.2 1.2.3 3.2.4	6.2	CT.PO-P1 CT.PO-P2	PT-4	PT-4		1 4(a)	6.2.a 6.2.c		164.506(b)(1) 164.508(a)(2) 164.508(a)(3) 164.510(b)(2)(i) 164.510(b)(2)(ii) 164.510(b)(2)(iii) 164.510(b)(3) 164.514(d)(2)(i) 164.514(f)(2)(iv) 164.514(f)(2)(v)		7002(e) 7002(f) 7012(e) 7012(f) 7020(d) 7012(e) 7012(f) 7012(g) 7012(h) 7012(i) 7012(j) 7012(k) 7012(l) 7012(m) 7012(n) 7012(o) 7012(p) 7012(q) 7012(r) 7027(d) 7027(e)	6-1-1306(1) 6-1-1306(1)(a)(I)(A) 6-1-1306(1)(a)(I)(B) 6-1-1306(1)(a)(IV) 6-1-1306(1)(a)(IV) (A) 6-1-1306(1)(a)(IV) (B) 6-1-1306(1)(a)(IV) (C)	15(b)(3)					5(2)(b) 5(2)(c)	47-18-3203(a)(2)(B) 47-18-3203(a)(2)(C) 47-18-3204(a)(B)			59.1-578.A.5 59.1-578.D		21.1 21.2 21.3 21.4 21.5 7.1 7.2 9.2(a)	10.1 15.1 24.1 25.1 25.2 25.3 5.1 5.1	APP Part 1	APP 3	4(1)(a) 4(1)(6)(ii) 6(7) 7(e) 8(3)(a) 8(8)(b)	Sec 6 Sec 7 Principle 3
2.2	Initial Consent	Prior to the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of the individual's personal data, the knowledge and consent of the individual are required.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject(s): (1) Receives notice of the organization's data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5		P2.2 P3.1 P3.2 P3.2-POF1 P3.2-POF2 P3.2-POF3 P3.2-POF4 P3.2-POF5 P3.2-POF6 P3.2 P3.2-POF2	2(e) 4(a) 5	1.2.1 1.2.2 1.2.3 3.2.4	6.2	CT.PO-P1 CT.PO-P2	PT-4	PT-4		1 4(a)	6.2.a 6.2.c		164.506(b)(1) 164.508(a)(2) 164.508(a)(3) 164.510(b)(2)(i) 164.510(b)(2)(ii) 164.510(b)(2)(iii) 164.510(b)(3) 164.514(d)(2)(i) 164.514(f)(2)(iv) 164.514(f)(2)(v)		7002(e) 7002(f) 7012(e) 7012(f) 7020(d) 7012(e) 7012(f) 7012(g) 7012(h) 7012(i) 7012(j) 7012(k) 7012(l) 7012(m) 7012(n) 7012(o) 7012(p) 7012(q) 7012(r) 7027(d) 7027(e)	6-1-1306(1) 6-1-1306(1)(a)(I)(A) 6-1-1306(1)(a)(I)(B) 6-1-1306(1)(a)(IV) 6-1-1306(1)(a)(IV) (A) 6-1-1306(1)(a)(IV) (B) 6-1-1306(1)(a)(IV) (C)	15(b)(3)					5(2)(b) 5(2)(c)	47-18-3203(a)(2)(B) 47-18-3203(a)(2)(C) 47-18-3204(a)(B)			59.1-578.A.5 59.1-578.D		21.1 21.2 21.3 21.4 21.5 7.1 7.2 9.2(a)	10.1 15.1 24.1 25.1 25.2 25.3 5.1 5.1	APP Part 1	APP 3	4(1)(a) 4(1)(6)(ii) 6(7) 7(e) 8(3)(a) 8(8)(b)	Sec 6 Sec 7 Principle 3
2.3	Updated Consent	Based on changes to data privacy practices that affect the parameters of an individual's initial consent, updated consent of the individual is required to: (1) Continue collecting, receiving, processing, storing, transmitting, sharing, updating and/or disposal of the individual's personal data. This is also referred to as the right to revoke or "opt out" at any time after the initial consent was provided.	Functional	Intersects With	Just-in-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to prevent data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose of their Personal Data (PD) from providing such consent, unless: (1) The original circumstances under which an individual gave consent have changed; or(2) A significant amount of time has passed since an individual gave consent.	5		P2.1 P2.1-POF4 P3.2				CT.PO-P1 CT.PO-P2	PT-4(2) PT-5(1)				8.14.b.i 8.14.b.ii			7002(f) 7012(f) 7020(d) 7020(f) 7020(h) 7020(i) 7027(b) 7027(c) 7210(b) 7220(b)	6-1-1306(1) 6-1-1306(1)(a)(I)(A) 6-1-1306(1)(a)(I)(B) 6-1-1306(1)(a)(IV) 6-1-1306(1)(a)(IV) (A) 6-1-1306(1)(a)(IV) (B) 6-1-1306(1)(a)(IV) (C)														APP 5		Sec 6 Sec 7 Principle 3
			Functional	Intersects With	Revoke Consent	PRI-03.4	Mechanisms exist to allow data subjects to revoke consent to collect, receive, process, store, transmit, share and/or update their Personal Data (PD).	5									PT-4(3)								6-1-1306(1) 6-1-1306(1)(a)(I)(A) 6-1-1306(1)(a)(I)(B) 6-1-1306(1)(a)(IV) 6-1-1306(1)(a)(IV) (A) 6-1-1306(1)(a)(IV) (B) 6-1-1306(1)(a)(IV) (C)		5(1)(d)			7.3	5.2			5(2)(b) 6(4) 6(7) 8(7)(a) 8(8)(b)	
2.4	Equal Service & Price	Implement business processes to protect the right of data subjects to equal service and price, even if they exercise their data privacy rights.	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		CC1.5 CC2.2 CC2.3 CC3.1-POF5 CC3.1-POF14 CC3.1-POF1 CC3.1-POF6 CC3.1-POF4	4.1 4.2(a) 4.2(b) 4.2(c)	6.12	GV.PO-P5 GV.MT-P3	PR.-1 PM-8	PL-1	GV.OC-03 GV.SC-01 PR			8.7.c 8.5.a 8.5.b.i		164.306(e) 164.308(a)(8)(1) 164.308(a)(8)(2) 164.314(b)(1) 164.314(a)(2)(iii) 164.504(g)(1)		7013(h) 7022(e) 7022(m) 7027(b) 7027(c) 7123(b)(3) 7200(a) 7200(b)	6-1-1302(1) 6-1-1303(5)(a) 6-1-1307(2) 6-1-1308(8)(a)			45(a) 45(c) 45(e) 45(d) 50		7(1)(b)		58.1-581.4			2.1 A5.5	APP Part 11		7(c) 7(e) 8(3) 8(4)	Principle 7
			Functional	Intersects With	Product or Service Delivery Restrictions	PRI-03.5	Mechanisms exist to prevent discrimination against a data subject for exercising their legal rights pertaining to modifying or revoking consent, including prohibiting:(1) Refusing products and/or services;(2) Charging different rates for goods and/or services; and(3) Providing different levels of quality.	5						updated in 2026.1 release							164.508(c)(2)(iii)(A) 164.508(c)(2)(iii)(B) 164.514(f)(2)(iii)		7008(a) 7008(b) 7210(f)	6-1-1308(3)(d)			5(2)(d)				58.1-572.1.E 58.1-578.A.5 58.1-578.A.6			7				
2.5	Prohibit The Sale of Personal Data	Provide a clear and conspicuous link on the organization's Internet-based homepage, titled "Do Not Sell My Personal Data" that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal data.	Functional	Intersects With	Tailored Consent	PRI-03.1	Mechanisms exist to allow data subjects to modify permission to collect, receive, process, store, transmit, share, update and/or dispose selected attributes of their Personal Data (PD).	5		P3.2-POF1					CT.PO-P3	PT-4(1)							6-1-1306(1) 6-1-1306(1)(a)(I)(A) 6-1-1306(1)(a)(I)(B) 6-1-1306(1)(a)(IV) 6-1-1306(1)(a)(IV) (A) 6-1-1306(1)(a)(IV) (B) 6-1-1306(1)(a)(IV) (C)				47-18-3203(a)(2)(B) (I) 47-18-3203(a)(2)(B) (II) 47-18-3203(a)(2)(C) (I) 47-18-3204(b)							
			Functional	Intersects With	Prohibition of Selling, Processing and/or Sharing Personal Data (PD)	PRI-03.3	Mechanisms exist to prevent the sale, processing and/or sharing of Personal Data (PD) when:(1) Instructed by the data subject; or(2) The data subject is a minor, where selling and/or sharing PD is legally prohibited.	5							CT.PO-P3 CT.PO-P5						164.502(e)(5)(ii)(A)			6-1-1306(1) 6-1-1306(1)(a)(I)(A) 6-1-1306(1)(a)(I)(B) 6-1-1306(1)(a)(IV) 6-1-1306(1)(a)(IV) (A) 6-1-1306(1)(a)(IV) (B) 6-1-1306(1)(a)(IV) (C)	15(c)		2.3		47-18-3203(a)(2)(B) (I) 47-18-3203(a)(2)(B) (II) 47-18-3203(a)(2)(C) (I) 47-18-3204(d)		59.1-577.1.C 59.1-578.A.5 59.1-578.A.7					APP 7		
2.6	Authorized Agent (Proxy)	Allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	Functional	Intersects With	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity (e.g., authorized agent, proxy, etc.), acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	5													8.2.b		164.502(g)(2) 164.502(g)(3) 164.502(g)(3)(i) 164.502(g)(3)(ii)(A)		7024(j) 7026(a) 7026(e) 7063(a)(1) 7063(a)(2) 7063(b) 7063(c) 7210(j)	6-1-1306(5)(b)(II)	15(b)(3)				4(4)	47-18-3203(e)(1)		59.1-577.1.D 59.1-577.A 59.1-578.A.5 59.1-578.A.7			8.1 A.2			14(3) 14(4) 9(1)	
2.7	Global Privacy Control (GPC)	Enable automated mechanisms to provide data subjects with functionality to automatically exercise pre-selected opt-out preferences (e.g., opt-out signal).	Functional	Intersects With	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	5															7025(a) 7025(b)(1) 7025(b)(2) 7025(b)(3) 7025(c)(1) 7025(c)(2) 7025(c)(3) 7025(c)(4) 7025(c)(5) 7025(c)(6) 7025(d) 7026(a) 7026(b) 7026(f)(1) 7026(f)(2) 7025(f)(3) 7026(g) 7027(g)(1) 7027(g)(2) 7027(g)(3)				5(5)(c) 5(5)(c)(A) 5(5)(c)(B) 5(5)(c)(C) 5(5)(c)(D)										
3	Limited Collection & Use	Ensure that the design of data collection and use are consistent with the expectations of the information and the need for new information is balanced against any data privacy risks.	Functional	Intersects With	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to what is necessary, as defined in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	5		CC6.1-POF18 P3.0 P3.1 P3.1-POF1 P3.1-POF2 P3.1-POF3 P3.1-POF4	3	4.1.2 9.2.2		6.4 6.5		PT-2	PT-2			4		45.48.410	7002(f)	6-1-1305(2)	15(b)	10(b)(i) 10(b)(ii)				5(1)(b) 5(2)(b)	47-18-2204(a)(1) 47-18-2204(a)(2)		59.1-578.A.1 59.1-578.A.5 59.1-578.A.7.a 59.1-578.A.7.c			5.3(b) 5.3(c) A.1		APP Part 3	APP 3		Principle 3 Principle 4 P1-C(1)(b) Principle 3 P1-C(2) P1-C(2)(a) P1-C(2)(b) P1-C(2)(c) P1-C(2)(d) P1-C(2)(e) P1-C(2)(f) P1-C(2)(g) P1-C(2)(h) P1-C(2)(i) P1-C(2)(j) P1-C(2) P1-C(3) P1-C(4) P1-C(4)(a) P1-C(4)(b) P1-C(4)(c) P1-C(4)(d) P1-C(4)(d)(i) P1-C(4)(d)(ii) P1-C(4)(e) P1-C(4)(f) P1-C(4)(g) P1-C(4)(h) P1-C(4)(i) P1-C(4)(j) P1-C(5) P1-C(6) P1-C(7) P1-C(8) P4-D(1) P4-D(2)	Sec 5 Principle 4
3.1	Authority To Collect	Identify the lawful basis given to collect, create, use, disseminate, maintain, and/or disclose an individual's personal data. Document this authority in the organization's publicly-facing data privacy notice.	Functional	Intersects With	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose of Personal Data (PD), either generally or in support of a specific business process.	5		CC6.1-POF18 P3.1 P4.1-POF1	4(c)	1.2.5 1.2.11 4.2.2		6.3	CT.DP-P4	PT-2	PT-2		1 4(b)	3		164.502(a)(1)(i) 164.502(a)(1)(ii) 164.502(a)(1)(iii) 164.502(a)(5)(i) 164.502(i)			6-1-1308(4)	15(b)	10(b)(i) 10(b)(ii)				5(2)(b)	47-18-2204(a)(5) 47-18-2204(b)		59.1-578.J.1.a 59.1-578.J.2.a	2403(a)(2)(A) 2403(a)(2)(B) 2403(a)(2)(C)		10 9.2(c) 9.2(d) 9.2(f) 9.2(g) 9.2(h) 9.2(i) 9.2(j) 9.2(l) 9.3	13.1	APP Part 3	APP 3 APP 7	4(1)(b)		Sec 5 Principle 4
3.2	Data Minimization	Take steps to minimize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of the individual's personal data that is directly relevant and necessary to accomplish a legally authorized purpose.	Functional	Intersects With	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business practices.	5								PM-25 SA-03(2) SA-03(3)	PM-25 SI-12(2) SA-8(33)							6-1-1308(3)										
		Restrict the internal use of personal data to only authorized purpose(s) that are consistent with the stated data privacy notice.		Intersects With	Minimize Sensitive / Regulated Data	DCH-18.1	Mechanisms exist to minimize sensitive/regulated data that is collected, received, processed, stored and/or transmitted throughout the information lifecycle to only those elements necessary to support necessary business processes.	5						6.5		SI-12(1)	SI-12(1)					164.502(b)(1)										11.3					
				Intersects With	Internal Use of Personal Data For Testing, Training & Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that:(1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and(2) Authorizes the use of PD when such information is required for internal testing, training and research.	5		CC6.1-POF13 P4.1		7.2.2 7.2.3 9.2.2			CT.PO-P1 CT.PO-P2	PM-25 PT-3 SI-12(1) SI-12(2)	PM-25 PT-3 SI-12(1) SI-12(2)						164.508(a)(2)(iii)(B)			6-1-1308(4)			2.3	7(3)(c)	A7-18-2204(a)(2) A7-18-2207(5)(C) A7-18-2207(5)(D) A7-18-2207(5)(E) A7-18-2207(6)(C) A7-18-2207(6)(D) A7-18-2207(6)(E) A7-18-2207(6)(F)(III) A7-18-2207(6)(F)(IV) A7-18-2207(6)(F)(V) A7-18-2207(6)(G)(I)								APP Part 3	APP 6		Principle 10 P10-(1) P10-(1)(a) P10-(1)(b)(i) P10-(1)(b)(ii) P10-(1)(c) P10-(1)(d) P10-(1)(e)(i) P10-(1)(e)(ii) P10-(1)(f)(i) P10-(1)(f)(ii) P10-(2)	

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	AICPA TSC 2017+2022 (used for SOC 2)	APEC Privacy Framework 2015	CAPP	ISO 27701 2025	ISO 29100 2024	NIST Privacy Framework 1.0	NIST 800-53 R5	NIST 800-53B R5 (privacy)	NIST CSF 2.0	OECD Privacy Principles	US Data Privacy Framework (DPF)	US FIPPS	US HIPAA Administrative Simplification Regulation	US - AK PIPA	US - CA CCPA 2025	US - CO Colorado Privacy Act	US - IL BIPA	US - IL IPA	US - IL PIPA	US - NV SB220	US - OR CPA	US - TN Tennessee Information Protection Act	US - TX SCUTI	US - VA CDPA 2023	US - VT Act 171 of 2018	EMEA EU GDPR	EMEA Saudi Arabia Personal Data Protection Law (PDPL)	APAC Australia Privacy Act	APAC Australian Privacy Principles	APAC India DPDPA 2023	APAC New Zealand Privacy Act of 2020	Americas Canada PIPEDA
3.3	Internal Use		Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and/or (3) What is consistent with applicable laws, regulations and contractual obligations.	5		P4.0 P4.1 P4.1-POF1		5.2.1 9.2.2			6.6	CT.DM-P8 CT.DP-P6 CT.PO-P2 CT.PO-P4	AC-23 PM-25 PT-2 PT-7	PM-25 PT-2 PT-7			4	8.2.c	4	164.510(a) 164.510(b)(1)(i) 164.510(b)(1)(ii) 164.510(b)(1)(iii) 164.510(b)(2) 164.510(b)(3) 164.512 164.512(a)(1) 164.512(a)(2) 164.512(b)(1)(i) 164.512(b)(1)(ii) 164.512(b)(1)(iii) 164.512(b)(1)(iii)(A) 164.512(b)(1)(iii)(B) 164.512(b)(2)(i) 164.512(b)(2)(ii) 164.512(b)(3) 164.512(b)(3)(i) 164.512(b)(3)(ii) 164.512(b)(3)(iii) 164.512(b)(3)(iv) 164.512(b)(3)(v) 164.512(b)(3)(vi) 164.512(c) 164.512(c)(1) 164.512(c)(2) 164.512(d) 164.512(d)(1) 164.512(d)(2) 164.512(d)(3) 164.512(d)(4) 164.512(d)(5) 164.512(e)(1)(i) 164.512(e)(1)(ii) 164.512(e)(1)(iii) 164.512(e)(1)(iv) 164.512(e)(1)(v) 164.512(e)(1)(vi)		7023(B)(3) 7026(f) 7028(7)(1) 7027(m)	6-1-1305(2) 6-1-1308(4) 6-1-1308(7)	15(b)(2)				2.3	4(7)(b) 5(2)(a)	47-18-3203(a)(2)(C) (D)(i) 47-18-3203(a)(2)(C) (ii) 47-18-3204(a)(6) 47-18-3205(c) 47-18-3207(c) 47-18-3207(d)	59-1-577.1.C 59-1-578.A.2 59-1-578.F.1.c		11.3	APP Part 3	APP 6 APP 7 APP 9	7(f) 7(g) 7(h) 7(i) 8(1)	Principle 10 P10-(1) P10-(1)(a) P10-(1)(a)(i) P10-(1)(a)(ii) P10-(1)(b) P10-(1)(b)(i) P10-(1)(b)(ii) P10-(1)(b)(iii) P10-(1)(c) P10-(1)(c)(i) P10-(1)(c)(ii) P10-(1)(d) P10-(1)(d)(i) P10-(2)	
4	Transparency	Provide a transparent notice to the public about data privacy practices through a data privacy notice(s) and other applicable privacy notices, as well as training and other digital services regarding the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of the personal data.	Functional	Intersects With	Privacy Act Statements	PRI-01.2	Mechanisms exist to provide additional formal notice to individuals from whom Personally Identifiable Information (PII) is solicited that: (1) Indicates the authority of organizations to collect Personal Data (PD); (2) Whether providing PD is mandatory or optional; (3) The principal purpose or purposes for which the PD is to be used; (4) The intended disclosures or routine uses of the information; and/or (5) The consequences of not providing all or some portion of the information requested.	5		P1.1		10.2.3				CM.PO-P1 CM.AW-P1	PT-5(2)	PT-5(2)																								
				Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals, prior to their data being collected, that is clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (2) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (3) Define the scope of PD collected, received, processed, stored, transmitted, shared, updated and disposed to third-parties; (4) Describe the purpose(s) that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5		CC2.3-POF7 P1.1 P1.1-POF1 P1.1-POF2 P1.1-POF3 P1.1-POF4 P1.1-POF5 P1.1-POF6 P1.1-POF7	2 2(a) 2(b) 2(c) 2(d) 2(e)	2.1.1 2.2.1 2.2.2 2.2.3 3.1.3 3.1.1 3.1.2 4.1.1 4.1.2 5.1.1 5.1.2 7.1.0 7.1.1 8.1.1 8.1.3 9.1.0 10.1.1 10.1.1 10.2.3			6.3	CM.PO-P1 CM.AW-P1	PM-20(1) PT-5	PM-20(1) PT-5			8.1.a.i 8.1.a.ii 8.1.a.iii 8.1.a.iv 8.1.a.v 8.1.a.vi 8.1.a.vii 8.1.a.viii 8.1.a.ix 8.1.a.x 8.1.a.xi 8.1.a.xii 8.1.b 8.1.c 8.11.d.i 8.11.d.ii 8.14.b.ii	3 8	164.520(b)(2)(iv) 164.520(b)(2)(v) 164.520(b)(2)(vi)(B) 164.520(c)(2)(ii) 164.520(c)(3) 164.520(d)(1)(ii) 164.520(d)(1)(iii) 164.520(d)(1)(iii)(A) 164.520(d)(1)(iii)(B) 164.520(d)(1)(iii)(C) 164.520(d)(1)(iv) 164.520(d)(1)(iv)(A) 164.520(d)(1)(iv)(B) 164.520(d)(1)(v) 164.520(d)(2)(i) 164.520(d)(2)(ii) 164.520(d)(2)(iii) 164.520(d)(3) 164.520(e) 164.520(e)(1)(i) 164.520(e)(1)(ii) 164.520(e)(1)(iii) 164.520(e)(1)(iv)		7011(e)(1)(F) 7011(e)(1)(G) 7011(e)(1)(H) 7011(e)(1)(I) 7011(e)(2) 7011(e)(2)(A) 7011(e)(2)(B) 7011(e)(2)(C) 7011(e)(2)(D) 7011(e)(2)(E) 7011(e)(2)(F) 7011(e)(2)(G) 7011(e)(2)(H) 7011(e)(2)(I) 7011(e)(3) 7011(e)(3)(A) 7011(e)(3)(B) 7011(e)(3)(C) 7011(e)(3)(D) 7011(e)(3)(E) 7011(e)(3)(F) 7011(e)(3)(G) 7011(e)(3)(H) 7011(e)(3)(I) 7011(e)(4) 7011(e)(5) 7012(a) 7012(a)(1) 7012(a)(2) 7012(a)(3) 7012(b) 7012(b)(1) 7012(b)(2) 7012(b)(3) 7012(c) 7012(d)	6-1-1309(2) 6-1-1308(5)(a) 6-1-1308(5)(b) 6-1-1308(5)(c)(I) 6-1-1308(5)(c)(II)(A) 6-1-1308(5)(c)(II)(B) 6-1-1308(5)(c)(II)(C) 6-1-1308(5)(d) 6-1-1308(5)(e) 6-1-1308(6) 6-1-1308(7) 6-1-1313(1)(m)	15(a)									5(3)(a) 5(4)(a) 5(4)(b) 5(4)(c) 5(4)(e) 5(4)(g) 5(4)(i) 5(4)(j)	47-18-3204(a)(1) 47-18-3208(c) 47-18-3204(c)(1) 47-18-3204(c)(2) 47-18-3204(c)(3) 47-18-3204(c)(4) 47-18-3204(c)(5) 47-18-3204(d) 47-18-3204(e)(1)	59-1-578.C 59-1-578.C.1 59-1-578.C.2 59-1-578.C.3 59-1-578.C.4 59-1-578.C.5 59-1-578.D 59-1-578.E 59-1-581.A.2		12.7 13.1(a) 13.1(b) 13.1(c) 13.1(d) 13.1(e) 13.2 13.2(d) 13.2(e) 13.2(f) 13.2(d) 13.2(e) 13.3 14.1(a) 14.1(b) 14.1(c) 14.1(d) 14.1(e) 14.1(f) 14.2 14.2(a) 14.2(b) 14.2(c) 14.2(d) 14.2(e) 14.2(f) 14.2(g) 14.3(a) 14.3(b) 14.3(c) 14.4 14.5(a)	12 12.1 12.4 13.5 13.6 4.1	APP Part 5	APP 1 APP 5	5(1)(i) 5(1)(ii) 5(2)(a)(i) 5(2)(a)(ii) 5(2)(a)(iii) 5(2)(b) 6(10)	Principle 3 P3-(1) P3-(1)(a) P3-(1)(a)(i) P3-(1)(c) P3-(1)(d) P3-(1)(e) P3-(1)(e)(i) P3-(1)(e)(ii) P3-(1)(e)(iii) P3-(1)(e)(iv) P3-(2) P3-(2)(a) P3-(2)(b) P3-(3) P3-(3)(a) P3-(3)(b) P3-(3)(c) P3-(4) P3-(4)(a) P3-(4)(b) P3-(4)(b)(i) P3-(4)(b)(ii) P3-(4)(b)(iii) P3-(4)(b)(iv) P3-(4)(c) P3-(4)(d) P3-(4)(e) P3-(4)(e)(i) P3-(4)(e)(ii)	Principle 2
				Intersects With	Notification of Disclosure Request To Data Subject	PRI-14.2	Mechanisms exist to notify data subjects of applicable legal requests to disclose Personal Data (PD).	5																									24.2						
4.1	Data Privacy Notice & Purpose Specification	Provide notice of the specific purpose(s) for which personal data is collected, created, used, disseminated, maintained, retained and/or disclosed.	Functional	Intersects With	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	5		P1.1-POF1 P1.1-POF2 P1.1-POF3 P1.1-POF4 P4.3-POF1		4.2.1		6.3	CM.PO-P1	PT-3	PT-3		3	8.1.a.iv 8.5.a	3 7	164.502(a)(3) 164.508(c)(1)(i) 164.508(c)(1)(ii) 164.508(c)(1)(iii) 164.508(c)(2)(i)(A) 164.508(c)(2)(i)(B)	7002(2)(a)(i) 7002(2)(a)(ii) 7002(2)(d) 7027(m)	6-1-1308(1)(a) 6-1-1308(1)(b)(I) 6-1-1308(1)(b)(II) 6-1-1308(1)(b)(III) 6-1-1308(1)(c) 6-1-1308(1)(d) 6-1-1308(2) 6-1-1313(1)(m)	15(b)(1) 15(b)(2)					5(1)(a) 5(4)(b) 5(4)(i)	47-18-3204(c)(2)	59-1-578.C.2		2447(a) 2447(a)(1) 2447(a)(1)(A) 2447(a)(1)(B) 2447(a)(1)(C) 2447(a)(2)(I) 2447(a)(2)	12.1(c) 14.1(c)	11.1 13.2 12.3	APP Part 3	APP 1	4(2) 5(14) 5(15)(a)(i) 8(8)(a)		Sec 5 Principle 2
				Intersects With	Notification of Disclosure Request To Data Subject	PRI-14.2	Mechanisms exist to notify data subjects of applicable legal requests to disclose Personal Data (PD).	5																									24.2						
5	Data Lifecycle Management	Limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of personal data to that which is legally authorized, relevant and deemed "reasonably necessary" for the proper performance of business functions.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5		A1.2-POF7 C1.1 C1.1-POF2 CC2.1 CC6.1 CC6.5 CC6.7-POF2 CC8.1-POF16 CC8.1-POF17 P3.1-POF1 P3.1-POF2 P3.1-POF3 P3.1-POF4			7.5.3(b)		GV.PO-P1	MP-1	MP-1	ID.AM-08 PR.DS-01 PR.DS-02 PR.DS-10		45.48.100		164.306(a)(3) 164.312(a)(1) 164.312(c)(1) 164.514(b)(2)(i)(E) 164.530(c)(2)(i)		6-1-1305(4) 6-1-1307(2) 6-1-1307(3) 6-1-1308(5)																Principle 7	
				Intersects With	Automated Data Management Processes	PRI-02.2	Automated mechanisms exist to adjust data that is able to be collected, received, processed, stored, transmitted, shared, updated and/or disposed, based on updated data subject authorization(s).	5							CT.DM-P7	PM-24 PT-2(2) PT-5(2)	PM-24																					
				Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destruct, 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		C1.1-POF3 C1.2 C1.2-POF1 C1.2-POF2 CC6.5-POF2 P4.2 P4.2-POF1 P4.3 P4.3-POF1 P4.3-POF2			5.2.2 5.2.3		6.5 6.6	CT.DM-P5	AC-4(25) SI-12 SI-12(3)	SI-12 SI-12(3)	ID.AM-07		45.48.500				8.5.b	4		7(2)(a) 7(2)(b) 7(2)(c) 7(2)(d) 7(2)(e) 7(2)(f) 7(2)(g)	47-18-3203(a)(2)(F) 47-18-3204(a)(4)	521.052(b)					15(a) 15(b)(2)			5.1(e)	11.4 18.1 18.2.a 18.2.b	APP Part 2 APP Part 6	APP 6 APP 8				Sec 7 Sec 8 Principle 5 Principle 6
				Intersects With	Data Tagging	PRI-11	Mechanisms exist to issue data modeling guidelines to support tagging of sensitive/regulated data.	5							CT.DM-P7	PT-3(1)																					
5.1	Processing Records	Maintain a record of processing activities that documents the organization's necessary records to support its obligations for the processing of sensitive/regulated data.	Functional	Intersects With	Personal Data (PD) Lineage	PRI-09	Mechanisms exist to maintain a process to document the lineage of Personal Data (PD) by recording how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes PD.	5							CM.AW-P4 CM.AW-P6	SA-4(12)																					
5.2	Data Flow Mapping	Maintain a record of processing activities that documents the flow of personal data that includes: - Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data; - Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data; - Purposes for which the data is transmission and processing; - A description of the categories of data subjects and personal data; - Where possible, the time limits for erasure of the different categories of data; and - Where possible, a description of the cybersecurity & data privacy measures of the data controller.	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	updated in 2026.1 release	CC2.1-POF6 CC5.1-POF1 CC6.1-POF1					ID.AM-P1	CM-8 PM-5		ID.AM-01 ID.AM-02 ID.AM-08				164.316(b)(2)(iii)		7123(c)(4) 7123(c)(4)(B)															
				Intersects With	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulated data is stored, transmitted or processed.	5	updated in 2026.1 release	CC2.1-POF5 CC2.1-POF9					ID.IM-P1 ID.IM-P4 ID.IM-P5 ID.IM-P6	CM-13								7123(c)(4)(A)													
				Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5		C1.1-POF1 CC2.1 CC2.1-POF2 CC2.1-POF5					ID.IM-P1	PL-2 SA-4(2) SA-4(2)	PL-2	ID.AM-03						7123(c)(4)(A)													
				Intersects With	Sensitive / Regulated Data Actions	CFG-06.1	Automated mechanisms exist to generate event logs whenever sensitive/regulated data is collected, created, updated, deleted and/or archived.	5													164.312(c)(2)															
				Intersects With	Sensitive / Regulated Media Records	DCH-01.2	Mechanisms exist to ensure media records for sensitive/regulated data contain sufficient information to determine the potential impact in the event of a data loss incident.	5										PR.DS																	
				Intersects With	Data Tagging	PRI-11	Mechanisms exist to issue data modeling guidelines to support tagging of sensitive/regulated data.	5							CT.DM-P7	PT-3(1)																					
5.3	Data Custodians	Identify the owners or operators of Technology Assets, Applications and/or Services (TAAS) that process data, or with which data subjects are interacting.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed from the time assets are procured and throughout the asset's lifecycle to establish a common understanding of requirements for asset protection.	5							ID.IM-P2	SA-4(12)		ID.AM				164.316(b)(2)(iii)													
				Intersects With	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.	5							ID.IM-P2	CM-8(6)		ID.AM				164.316(b)(2)(iii)													
5.4	Retention of Personal Data	Ensure that all records containing personal data are maintained in accordance with the organization's records retention schedule and comply with applicable statutory, regulatory and contractual obligations.	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		C1.1-POF3 P4.3						SI-12 SI-12(3)	SI-12					164.316(b)(2)(i)		7123(g) 7123(i)(7)(E) 7155(1)			8(6)									8(7)(a) 8(8)		
				Intersects With	Minimize Sensitive / Regulated Data	DCH-18.1	Mechanisms exist to minimize sensitive/regulated data that is collected, received, processed, stored and/or transmitted throughout the information lifecycle to only those elements necessary to support necessary business processes.	5							6.5			SI-12(1) SI-12(1)				164.502(b)(1)					2.3			11.3								
5.5	Secure Destruction of Personal Data	Utilize secure methods to dispose of or destroy both physical and digital media that contains personal data.	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5		P4.3					CT.DM-P5	MP-6 MP-6(3)	MP-6				45.48.500	7122(c)(4)												8(7)(a)		
				Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5		C1.2 C1.2-POF1 C1.2-POF2 CC6.5 CC6.5-POF2 P4.3 P4.3-POF2 P4.3-POF3					CT.DM-P5	SI-12(3)	SI-12(3)			45.48.500 45.48.510															
				Intersects With	Information Location	DCH-24	Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.	5		CC2.1-POF9						CM-12																		Sec 20	
5.6	Geolocation Restrictions	Restrict the location of processing, storage and service locations to comply with the data privacy notice, as well as applicable statutory, regulatory and contractual obligations.	Functional	Intersects With	Transfer of Sensitive and/or Regulated Data	DCH-25	Mechanisms exist to restrict and govern the transfer of sensitive and/or regulated data to third-countries or international organizations.	5																												
				Intersects With	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	5								PE-23 SI-4																		Sec 20	
				Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		CC9.2-POF6 CC9.2						PE-23 SA-9(5)		GV.SC-06						7122(c)(1)(I)												Sec 20	
5.7	Data Portability	Provide the functionality to export personal data in a structured, commonly-used and machine-readable format that can be transferred to another controller without hindrance.	Functional	Intersects With	Data Portability	PRI-06.6	Mechanisms exist to format exports of Personal Data (PD) in a structured, machine-readable format that allows data subjects to transfer their PD to another controller without hindrance.	5		P6.7-POF2					CT.DM-P2 CT.DM-P6							164.524(c)(2)(ii) 164.524(c)(2)(iii)		7024(g)	6-1-1306(1)(e)					59-1-577.A.4		20.1						
				Intersects With	Personal Data (PD) Exports	PRI-06.7	Mechanisms exist to export a data subject's available Personal Data (PD) in a readily usable format, upon an authenticated request.	5		P6.7-POF2	8(a) 8(b) 8(b)(i) 8(b)(ii) 8(b)(iii) 8(b)(iv)				CT.DM-P2 CT.DM-P6				7(b) 7(b)(ix)						7024(g)	6-1-1306(1)(e)					59-1-577.A.4		20.1 20.1(b)(ii)				11(1)(a)		

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
5.8	Record of Disclosures	Develop and maintain an accounting of personal data disclosures that upon request can be made available to the individual whose personal data was disclosed.	Functional	Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	5	
				Intersects With	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	5	
5.9	Integrity Protections	Maintain the accuracy and relevance of personal data across the information lifecycle as personal data is collected, created, used, disseminated, maintained, retained and/or disclosed.	Functional	Intersects With	Data Governance	GOV-10	Mechanisms exist to facilitate data governance to oversee the organization's policies, standards and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	5	
				Intersects With	Personal Data (PD) Accuracy & Integrity	PRI-05.2	Mechanisms exist to ensure the accuracy and relevance of Personal Data (PD) throughout the information lifecycle by:(1) Keeping PD up-to-date; and(2) Remediating identified inaccuracies, as necessary.	5	
5.10	De-Identification	Process personal data in such a manner that it is not attributable to a data subject through technical or organizational measures (e.g., anonymization, pseudonymization or data minimization).	Functional	Intersects With	De-Identification (Anonymization)	DCH-23	Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.	5	
				Intersects With	Data Masking	PRI-05.3	Mechanisms exist to mask sensitive/regulated data through data anonymization, pseudonymization, redaction or de-identification.	5	
5.11	Quality Management	Maintain quality assurances throughout the information lifecycle with such accuracy, relevance, timeliness and completeness as is reasonably necessary to ensure fairness to the individual.	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	
				Intersects With	Data Quality Automation	PRI-10.1	Automated mechanisms exist to support the evaluation of data quality across the information lifecycle.	5	
5.12	Secure Data Processing	Implement secure data processing practices so that the confidentiality, integrity and pertinent attributes of sensitive/regulated data is maintained throughout the data lifecycle.	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	
				Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
				Intersects With	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.	5	
				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	
				Intersects With	Manage Organizational Knowledge	PRM-08	Mechanisms exist to manage the organizational knowledge of the security, compliance and resilience staff.	5	
				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	
				Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
5.13	Data Lineage	Maintain records of the inputs, entities and associated Technology Assets, Applications and/or Services (TAAS) that influence data of interest, providing a historical record of the data and its origins.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) 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 (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes.	5	
				Intersects With	Personal Data (PD) Lineage	PRI-09	Mechanisms exist to maintain a process to document the lineage of Personal Data (PD) by recording how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes PD.	5	- updated in 2026.1 release
5.14	Updated Use Permissions	Implement data management processes to adjust data that is able to be collected, created, used, disseminated, maintained, retained and/or disclosed, based on updated data subject authorization(s).	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when:(1) The original circumstances under which an individual gave consent have changed; or(2) A significant amount of time has passed since an individual gave consent.	5	
5.15	Flaw Remediation with Personal Data	Identify and correct flaws related to personal data as it is collected, created, used, disseminated, maintained, retained and/or disclosed.	Functional	Intersects With	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	5	
				Intersects With	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.	5	- updated in 2026.1 release
				Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	- updated in 2026.1 release
				Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	- updated in 2026.1 release
				Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	- updated in 2026.1 release
				Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	- updated in 2026.1 release
				Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	- updated in 2026.1 release
				Intersects With	Flaw Remediation with Personal Data (PD)	VPM-04.2	Mechanisms exist to identify and correct flaws related to the collection, usage, processing or dissemination of Personal Data (PD).	5	
				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	- updated in 2026.1 release
5.16	Analytical Biases	Understand and evaluate data analytic inputs and outputs for potential bias.	Functional	Intersects With	Data Analytics Bias	PRI-10.2	Mechanisms exist to evaluate its analytical processes for potential bias.	5	
		Provide data subjects with appropriate access to their personal data.		Intersects With	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).	5	- updated in 2026.1 release

SCF #	AICPA TSC 2017:2022 (used for SOC 2)	APEC Privacy Framework 2015	GAPP	ISO 27701 2025	ISO 29100 2024	NIST Privacy Framework 1.0	NIST 800-53 R5	NIST 800-53B R5 (privacy)	NIST CSF 2.0	OECD Privacy Principles	US Data Privacy Framework (DPF)	US FIPPS	US HIPAA Administrative Simplification 2013	US - AK PIPA
PRI-14	CC2.3 P8.1-POF4 P8.1-POF5		10.2.3 10.2.5			CM.AW-P4 CM.AW-P6 CM.AW-P7	PM-27	PM-27						
PRI-14.1	P6.2 P6.2-POF1 P6.3 P6.3-POF1		7.2.1 7.2.4			CM.AW-P4	PM-21	PM-21					164.528(a)(1)(ii) 164.528(a)(1)(iii) 164.528(a)(1)(iv) 164.528(a)(1)(ix) 164.528(a)(1)(v) 164.528(a)(1)(vi) 164.528(a)(1)(vii) 164.528(a)(1)(viii) 164.528(b) 164.528(b)(1) 164.528(b)(2) 164.528(b)(2)(i) 164.528(b)(2)(ii) 164.528(b)(2)(iii) 164.528(b)(2)(iv) 164.528(b)(3) 164.528(b)(3)(i) 164.528(b)(3)(ii) 164.528(b)(3)(iii) 164.528(b)(4)(i) 164.528(b)(4)(i)(A) 164.528(b)(4)(i)(B) 164.528(b)(4)(i)(C) 164.528(b)(4)(i)(D) 164.528(b)(4)(i)(E) 164.528(b)(4)(i)(F) 164.528(b)(4)(ii) 164.528(c)(1) 164.528(c)(1)(i) 164.528(c)(1)(ii) 164.528(c)(1)(ii)(A) 164.528(c)(1)(ii)(B) 164.528(c)(2) 164.528(d) 164.528(d)(1)	
GOV-10	CC1.2-POF1						PM-23 PM-24	PM-24						
PRI-05.2		6	9.2.1		6.7	PR.DS-P6	PM-24	PM-24			II.5.a			
DCH-23							SI-19	SI-19			III.14.a.i III.14.g.i			
PRI-05.3							SI-19(4)							
PRI-10	P7.0 P7.1 P7.1-POF1 P7.1-POF2		9.2.1			CT.PO-P4 CT.DM-P8	PM-22 PM-23 PM-24	PM-24		2		5	164.512(i)(1)(i)(B) 164.512(i)(1)(i)(B)(1) 164.512(i)(1)(i)(B)(2) 164.512(i)(1)(i)(B)(3)	
PRI-10.1							PT-3(2)							
PRM-04	CC3.1 CC4.1 CC5.2					CM.AW-P3 CT.PO-P1 CT.DM-P1 CT.DM-P2 CT.DM-P3 CT.DM-P4 CT.DM-P5 CT.DM-P6 CT.DM-P7 CT.DM-P8 CT.DM-P9 CT.DM-P10 CT.PO-P4	CA-2	CA-2						
PRM-05	CC2.2 CC4.1 CC5.2 PI1.1-POF1 PI1.1-POF2 PI1.1-POF3			6.1.1		CT.PO-P1 CT.DM-P9 CT.DM-P10	RA-9						164.306(b)(2)(ii)	
PRM-06	CC1.3 CC3.1 CC3.1-POF10 CC3.1-POF11 CC3.1-POF12 CC3.1-POF13 CC3.1-POF14 CC3.1-POF15 CC3.1-POF16 CC3.1-POF7 CC3.1-POF8 CC3.1-POF9 CC3.4 CC4.1 CC5.1 CC5.2 P6.7-POF1 PI1.1 PI1.1-POF1 PI1.3-POF1 PI1.3-POF2 PI1.3-POF3 PI1.3-POF4 PI1.3-POF5 PI1.4-POF1 PI1.4-POF2 PI1.4-POF3 PI1.4-POF4 PI1.5-POF1 PI1.5-POF2 PI1.5-POF3 PI1.5-POF4			4.1 4.2 4.2(a) 4.2(b) 4.2(c) 6.1.1		ID.IM-P5 CT.PO-P1 CT.DM-P9 CT.DM-P10	PM-11						164.306(b)(2)(i)	
PRM-07	CC5.2 CC8.1 CC8.1-POF1					CM.AW-P3 CT.PO-P1 CT.DM-P7 CT.DM-P8 CT.PO-P4	SA-3 SA-3(1) SA-8(30)	SA-3	GV.SC-09 ID.AM-08 PR.PS-02 PR.PS-03					
PRM-08						CT.PO-P1 CT.DM-P7 CT.DM-P8								
SEA-01	CC2.2 CC3.2 CC5.1 CC5.2 CC6.1-POF2 CC8.1-POF15 CC8.1-POF18		4.2.3 6.2.2 7.2.2 7.2.3			ID.DE-P4 GV.PO-P2 CT.PO-P1 CT.DM-P7 CT.DM-P8 CM.AW-P3	PT-1 SA-8 SC-1 SC-7(18) SI-1 SA-15(5)	PT-1 SI-1	PR.IR PR.IR-01 PR.IR-03		II.4.a		164.306(b)(1)	
TDA-06	PI1.1 PI1.2 PI1.2-POF1 PI1.2-POF2 PI1.2-POF3 PI1.3 PI1.3-POF1 PI1.3-POF2 PI1.3-POF3 PI1.3-POF4 PI1.3-POF5 PI1.4 PI1.4-POF1 PI1.4-POF2 PI1.4-POF3 PI1.4-POF4 PI1.5 PI1.5-POF1 PI1.5-POF2 PI1.5-POF3 PI1.5-POF4					CT.PO-P1 CT.DM-P7 CT.DM-P8 CT.DM-P9 CT.DM-P10	SA-1 SA-4(3) SA-15	SA-1	PR.PS-06					
IAO-03	CC2.2-POF11 CC2.3-POF10 CC2.3-POF11 CC2.3-POF9					ID.IM-P7 ID.IM-P8 ID.BE-P3 CM.AW-P6 PR.PO-P4	PL-2	PL-2						
PRI-09						CM.AW-P4 CM.AW-P6	SA-4(12)							
PRI-03.2	P2.1 P2.1-POF4 P3.2					CT.PO-P1 CT.PO-P3	PT-4(2) PT-5(1)				III.14.b.i III.14.b.ii			
DCH-22.1	P5.1 P5.2		6.2.5 6.2.6 10.2.1 10.2.2			CT.DM-P3	SI-18(4) SI-18(5)	SI-18(4)					164.526(a)(1) 164.526(b)(1)	
THR-06							RA-5(11)							
VPM-01	CC3.2-POF7 CC3.2-POF9 CC3.4-POF6 CC8.1-POF14 CC8.1-POF16 CC9.2-POF13					PR.PO-P10	SI-2 SI-3		ID.RA-01 ID.RA-08 PR.PS-02					
VPM-01.1	CC2.2-POF9 CC3.2-POF7 CC3.2-POF9 CC3.4-POF6 CC9.2-POF13						SA-11(6) SA-11(7)		PR.PS-02					
VPM-02	CC4.2 CC5.3-POF4 CC7.4-POF8						PM-4 SC-18(1)		ID.RA-08 PR.PS-02					
VPM-03	CC3.4-POF6								ID.RA-08					
VPM-04	CC4.2						SC-18(1)							
VPM-04.2														
VPM-05	CC8.1-POF14 CC8.1-POF16						SI-2 SI-2(4) SI-3		PR.PS-02					
PRI-10.2						ID.RA-P2								
PRI-03.7					6.5					1	II.2.c III.12.a III.12.b			

SCF #	US - CA CCPA 2025	US - CO Colorado Privacy Act	US - IL BIPA	US - IL IPA	US - IL PIPA	US - NV SB220	US - OR CPA	US - TN Tennessee Information Protection Act	US - TX BC521	US - VA CDPA 2025	US - VT Act 171 of 2018	EMEA EU GDPR	EMEA Saudi Arabia Personal Data Protection Law (PDPL)	APAC Australia Privacy Act	APAC Australian Privacy Principles	APAC India DPDPA 2023	APAC New Zealand Privacy Act of 2020	Americas Canada PIPEDA
PRI-14												30.1 30.1(a) 30.1(b) 30.1(c) 30.1(d) 30.1(e) 30.1(f) 30.1(g) 30.2 30.2(a) 30.2(b) 30.2(c) 30.2(d) 30.3	31 31.1 31.2 31.3 31.4 31.5 31.6					
PRI-14.1							3(1)(a)(B)(i) 3(1)(a)(B)(ii)									11(1)(b)		
GOV-10																		
PRI-05.2												5.1(d)	14	APP Part 10	APP 10	8(3) 8(3)(a) 8(3)(b)	Principle 9	Principle 6
DCH-23		6-1-1307(1)(a) 6-1-1307(1)(b) 6-1-1307(1)(b)(I)(A) 6-1-1307(1)(b)(I)(B) 6-1-1307(1)(b)(II) 6-1-1307(1)(b)(III)					7(1)(a)(A)	47-18-3203(a)(2)(C)		59.1-581.A.1								
PRI-05.3	7123(c)(5)(C)									59.1-581.A.1				APP Part 2				
PRI-10	7023(c)																	
PRI-10.1																		
PRM-04																		
PRM-05	7100(b)	6-1-1308(1)(c)(I) 6-1-1308(1)(c)(II)																
PRM-06		6-1-1308(1)(c)(I) 6-1-1308(1)(c)(II)																
PRM-07																		
PRM-08																		
SEA-01	7123(c)(5)(B)	6-1-1305(4) 6-1-1308(5)							521.052		2447(a) 2447(a)(1) 2447(a)(1)(A) 2447(a)(1)(B) 2447(a)(1)(C) 2447(a)(1)(D) 2447(a)(2)			APP Part 8 APP Part 11				Principle 7
TDA-06	7123(c)(14)																	
IAO-03																		
PRI-09																		
PRI-03.2	7002(f) 7010(f) 7022(g) 7022(h) 7025(c)(5) 7026(k) 7027(l) 7221(i) 7221(k)	6-1-1306(1) 6-1-1306(1)(a)(I)(A) 6-1-1306(1)(a)(I)(B) 6-1-1306(1)(a)(I)(C) 6-1-1306(1)(a)(II) 6-1-1306(1)(a)(III) 6-1-1306(1)(a)(IV)(A) 6-1-1306(1)(a)(IV)(B) 6-1-1306(1)(a)(IV)(C)													APP 5			Sec 6 Sec 7 Principle 3
DCH-22.1	7023(c)	6-1-1306(1)(c)								59.1-577.A.2			17.1	APP Part 13	APP 13		P6-(2) Principle 7 P7-(1) P7-(2) P7-(3)(a) P7-(3)(b) P7-(4) P7-(5) P7-(6)	Principle 10
THR-06	7123(c)(6)																	
VPM-01	7123(c)(5)(D) 7123(c)(6)										2447(c)(7)							
VPM-01.1	7123(c)(5)(D)																	
VPM-02	7123(c)(5)(D)																	
VPM-03	7123(c)(5)(D)																	
VPM-04	7123(c)(5)(D)																	
VPM-04.2																		
VPM-05	7123(c)(5)(A) 7123(c)(5)(D)										2447(c)(7)							
PRI-10.2																		
PRI-03.7	7010(e) 7010(f) 7025(c)(4) 7027(b) 7027(i)						3(1)(d)(A) 3(1)(d)(B) 3(1)(d)(C) 5(6)	47-18-3203(b)		59.1-577.A 59.1-577.A.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	AICPA TSC 2017:2022 (used for SOC 2)	APEC Privacy Framework 2015	GAPP	ISO 27701 2025	ISO 29100 2024	NIST Privacy Framework 1.0	NIST 800-53 R5	NIST 800-53B R5 (privacy)	NIST CSF 2.0	OECD Privacy Principles	US Data Privacy Framework (DPF)	US FIPPS	US HIPAA Administrative Simplification 2013	US - AK PIPA	US - CA CCPA 2025	US - CO Colorado Privacy Act	US - IL BIPA	US - IL IPA	US - IL PIPA	US - NV SB220	US - OR CPA	US - TN Tennessee Information Protection Act	US - TX BC521	US - VA CDPA 2025	US - VT Act 171 of 2018	EMEA EU GDPR	EMEA Saudi Arabia Personal Data Protection Law (PDPL)	APAC Australia Privacy Act	APAC Australian Privacy Principles	APAC India DPDPA 2023	APAC New Zealand Privacy Act of 2020	Americas Canada PIPEDA
6	Data Subject Rights		Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5) Request correction to their PD due to inaccuracies;(6) Request erasure of their PD; and(7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5		P5.0 P5.1 P5.1-POF1 P5.1-POF2 P5.1-POF3	8(c)	6.2.1 6.2.2 6.2.3 6.2.4 6.2.5 6.2.6		6.9 6.10	CT.DM-P1	AC-3(14) SI-18(4)	AC-3(14) SI-18(4)		7(a)	II.6.a III.14.e.ii III.8.a.i III.8.a.i.1 III.8.a.i.2 III.8.a.i.3 III.8.a.iii III.8.b.i III.8.b.ii III.8.d.ii III.8.d.ii III.8.e.i III.8.f.i	1 6	164.514(h)(1)(i) 164.514(h)(1)(ii) 164.524(a)(1) 164.524(a)(1)(i) 164.524(a)(1)(ii) 164.524(a)(1)(iii) 164.524(a)(1)(iii)(A) 164.524(a)(1)(iii)(B) 164.524(a)(2) 164.524(a)(2)(i) 164.524(a)(2)(ii) 164.524(a)(2)(iii) 164.524(a)(2)(iv) 164.524(a)(2)(v) 164.524(a)(3) 164.524(a)(3)(i) 164.524(a)(3)(ii) 164.524(a)(3)(iii) 164.524(a)(4) 164.524(b)(1) 164.524(b)(2)(i) 164.524(b)(2)(i)(A) 164.524(b)(2)(i)(B) 164.524(b)(2)(ii) 164.524(b)(2)(ii)(A) 164.524(b)(2)(ii)(B) 164.524(c) 164.524(c)(1) 164.524(c)(3)(i) 164.524(c)(3)(ii) 164.524(c)(4) 164.524(c)(4)(i) 164.524(c)(4)(ii) 164.524(c)(4)(iii) 164.524(c)(4)(iv) 164.524(d)		7020(a) 7020(b) 7020(c) 7020(d) 7020(e) 7020(f) 7020(f)(1) 7020(f)(2) 7022(b) 7023(c) 7023(d)(1) 7024(g) 7024(h) 7024(j) 7027(d) 7027(e)	6-1-1306(1)(b)				2.1	3(1)(a)(A)	47-18-3203(a)(1) 47-18-3203(a)(2)(A)		59.1-577.A 59.1-577.A.1 59.1-577.A.2 59.1-577.A.3 59.1-577.A.4		12.3 12.5(b) 12.6 15.1 15.1(a) 15.1(b) 15.1(c) 15.1(d) 15.1(e) 15.1(g) 15.1(h) 15.2 15.3 15.4 16 17.1 17.1 18.1 18.1(a) 18.1(b) 18.1(c) 18.1(d)	21 4.2 4.3 4.4 4.5	APP Part 12	APP 12	11(1)(c) 11(2)	Principle 6 P6-(1) P6-(1)(a) P6-(1)(b) P6-(2) P6-(3)	Principle 8 Principle 9
				Intersects With	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	5		P5.1-POF4 P5.2-POF1 P5.2-POF3					CT.DM-P1							164.524(d)(2)(i) 164.524(d)(2)(ii) 164.524(d)(2)(iii) 164.524(d)(3)		7022(a) 7023(b) 7024(a) 7024(b) 7026(e)	6-1-1306(1)					4(5)(e)(B)	47-18-3203(b)(4)										
6.1	Inquiry Management	Maintain a capability to receive and respond to data privacy-related requests, complaints, concerns or questions from data subjects.	Functional	Intersects With	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	5		P5.1 P5.2		6.2.5 6.2.6 10.2.1 10.2.2			CT.DM-P3	SI-18(4) SI-18(5)	SI-18(4)					164.526(a)(1) 164.526(b)(1)		7023(c)	6-1-1306(1)(c)								59.1-577.A.2			17.1	APP Part 13	APP 13		P6-(2) Principle 7 P7-(1) P7-(2) P7-(3)(a) P7-(3)(b) P7-(4) P7-(5) P7-(6)	Principle 10
				Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5		P4.3-POF1 P5.1 P5.1-POF4 P5.1-POF5 P5.2 P5.2-POF1 P5.2-POF3 P5.2-POF4 P6.7-POF2 P8.1 P8.1-POF1 P8.1-POF2 P8.1-POF3		6.2.5 6.2.6 7.1.2 10.2.1 10.2.2		6.10	GV.MT-P4 GV.MT-P7 CM.AW-P2 CT.PO-P4	PM-26	PM-26		7(b)(i) 7(b)(ii) 7(b)(iii) 7(c) 7(d)	II.7.a.i III.11.d.i III.8.i.i	6	164.526(b)(2)(i) 164.526(b)(2)(i)(A) 164.526(b)(2)(i)(B) 164.526(b)(2)(ii) 164.526(b)(2)(ii)(A) 164.526(b)(2)(ii)(B) 164.526(d) 164.526(d)(1) 164.526(d)(1)(i) 164.526(d)(1)(ii) 164.526(d)(1)(iii) 164.526(d)(1)(iv) 164.526(d)(2) 164.526(d)(3) 164.526(d)(4) 164.526(d)(5)(i) 164.526(d)(5)(ii) 164.526(d)(5)(iii) 164.526(e) 164.526(f) 164.530(d)(1) 164.530(d)(2)		7021(b) 7022(e) 7022(f) 7022(f)(1) 7023(a) 7023(d)(2)(A) 7023(d)(2)(B) 7023(d)(2)(C) 7023(d)(2)(D) 7023(f)(1) 7023(f)(2) 7023(f)(3) 7023(f)(4) 7023(i) 7023(j) 7023(k) 7024(c) 7024(c)(1) 7024(c)(2) 7024(c)(3) 7024(c)(4) 7024(d) 7024(d)(1) 7024(d)(2) 7024(e) 7024(e)(1) 7024(e)(2) 7024(k) 7024(k)(1) 7024(k)(2) 7024(k)(3) 7024(k)(4) 7024(k)(5) 7024(k)(6) 7027(h)	6-1-1306(2)(a) 6-1-1306(2)(b) 6-1-1306(2)(c) 6-1-1306(2)(d)				2.1 2.2 2.4	4(5)(a) 4(5)(b) 4(5)(c) 4(5)(d) 4(5)(e) 4(5)(e)(A) 4(5)(e)(B) 4(6)(b) 4(6)(c) 4(6)(d) 5(5)(a)(A) 5(5)(a)(B) 5(5)(a)(C) 5(5)(b) 5(5)(b)	47-18-3203(b)(1) 47-18-3203(b)(2) 47-18-3203(b)(3) 47-18-3203(b)(4) 47-18-3204(e)(1)(A) 47-18-3204(e)(1)(B) 47-18-3204(e)(1)(C) 47-18-3204(e)(2) 47-18-3207(b)(3) 47-18-3207(b)(3)(A) 47-18-3207(b)(3)(B) 47-18-3207(b)(3)(C)		59.1-577.B.1 59.1-577.B.2 59.1-577.B.3 59.1-577.B.4 59.1-577.C		12.4		APP Part 13	APP 12 APP 13			
				Intersects With	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	5	- updated in 2026.1 release															7060(a) 7060(b) 7060(c) 7060(c)(1) 7060(c)(2) 7060(c)(3) 7060(c)(3)(A) 7060(c)(3)(B) 7060(c)(3)(C) 7060(c)(3)(D) 7060(c)(3)(E) 7060(c)(3)(F) 7060(d) 7060(e) 7060(f) 7060(g) 7060(h) 7061(a) 7061(b) 7062(a) 7062(b) 7062(c) 7062(d) 7062(f) 7062(g)																	
				Intersects With	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	5		P5.1-POF4 P5.2-POF1 P5.2-POF3					CT.DM-P1							164.524(d)(2)(i) 164.524(d)(2)(ii) 164.524(d)(2)(iii) 164.524(d)(3)		7022(a) 7023(b) 7024(a) 7024(b) 7026(e)	6-1-1306(1)					4(5)(e)(B)	47-18-3203(b)(4)										
6.2	Updating Personal Data	Provide data subjects with appropriate opportunity to correct or amend their personal data.	Functional	Intersects With	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	5		P5.1 P5.2		6.2.5 6.2.6 10.2.1 10.2.2			CT.DM-P3	SI-18(4) SI-18(5)	SI-18(4)					164.526(a)(1) 164.526(b)(1)		7023(c)	6-1-1306(1)(c)								59.1-577.A.2			17.1	APP Part 13	APP 13		P6-(2) Principle 7 P7-(1) P7-(2) P7-(3)(a) P7-(3)(b) P7-(4) P7-(5) P7-(6)	Principle 10
				Intersects With	Updating Personal Data (PD) Process	PRI-12	Mechanisms exist to identify and record:(1) The process(es) used to update Personal Data (PD); and(2) The frequency that such updates occur.	5		P5.2 P5.2-POF2					CT.DM-P3							164.526(a)(1) 164.526(b)(1) 164.526(e) 164.526(f)		7023(b) 7023(b)(1) 7023(b)(1)(A) 7023(b)(1)(B) 7023(b)(1)(C) 7023(b)(2)					2.3							17.1					
6.3	Redress	Provide data subjects with appropriate opportunity to challenge the organization's compliance with its data privacy principles.	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for:(1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and(2) Disseminating corrections or amendments of PD to other authorized users of the PD.	5		P5.2 P5.2-POF2	8(c)	6.2.5 6.2.6 10.2.1 10.2.2		6.9	CM.AW-P8 CT.DM-P3	SI-18(4) SI-18(5)	SI-18(4)			II.6.a	1	164.526(a)(1) 164.526(a)(2) 164.526(a)(2)(i) 164.526(a)(2)(ii) 164.526(a)(2)(iii) 164.526(a)(2)(iv) 164.526(b)(1)		7023(a) 7023(b) 7023(d)(1) 7023(d)(2)	6-1-1306(1)(c)					3(1)(b)	47-18-3203(a)(2)(B)		59.1-577.A.2				APP Part 13	APP 13	12(1) 12(2)(a) 12(2)(b)	P6-(2) Principle 7 P7-(1) P7-(2) P7-(3)(a) P7-(3)(b) P7-(4) P7-(5) P7-(6)	Principle 10
6.4	Notice of Correction or Amendment	Notify affected data subjects and applicable third-parties when personal data is corrected or amended.	Functional	Intersects With	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected, amended or deleted.	5		P3.1-POF4 P5.2 P5.2-POF2 P5.2-POF3					CM.AW-P1 CM.PO-P1 CT.PO-P4	SI-18(5)						164.526(c) 164.526(c)(1) 164.526(c)(2) 164.526(c)(3) 164.526(c)(3)(i) 164.526(c)(3)(ii)		7022(e) 7023(f)							47-18-3203(b)(1)						APP Part 13	APP 13		P6-(2)	
				Intersects With	Obligation To Inform Third-Parties	PRI-07.3	Mechanisms exist to inform applicable third-parties of any modification, deletion or other change that affects shared Personal Data (PD).	5							CM.AW-P5 CM.AW-P7									7022(b)(2) 7022(b)(3) 7022(f)(4) 7023(c) 7026(f)(2) 7027(g)(2) 7027(g)(3)									59.1-579.B.2								
6.5	Appeal	Provide data subjects with appropriate opportunity to appeal an adverse decision to have incorrect personal data amended.	Functional	Intersects With	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	5		P5.2					CM.AW-P8	PM-26	PM-26					164.524(d)(4)		7023(d)(1) 7023(f)(3)	6-1-1306(3)(a) 6-1-1306(3)(b) 6-1-1306(3)(c)					4(6)(a)	47-18-3203(c)		59.1-577.C								Sec 11
6.6	Right to Erasure	Provide data subjects with appropriate opportunity to request the deletion of personal data where it is used, disseminated, maintained, retained and/or disclosed, including where the personal data is stored or processed by third-parties.	Functional	Intersects With	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5		P4.3-POF1					CT.DM-P4									7022(b)(1) 7022(f)(2)	6-1-1306(1)(d)					3(1)(c)	47-18-3203(a)(2)(C) 47-18-3203(a)(2)(C)(i)(a) 47-18-3203(a)(2)(C)(i)(b) 47-18-3203(a)(2)(C)(ii)		59.1-577.A.3		17.1(a) 17.1(b) 17.1(c) 17.1(d) 17.1(e) 17.1(f) 17.2 17.3 17.3(a) 17.3(b) 17.3(c) 17.3(d) 17.3(e)				12(1) 12(3) 8(7)(a)		
7	Cybersecurity by Design	Establish administrative, technical and physical safeguards to protect sensitive/regulated data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, Secure Controls Framework (SCF), etc.).	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	5		CC2.1-POF1 CC2.1-POF2 CC2.1-POF3 CC2.1-POF4 CC3.1-POF5 CC5.1 CC5.1-POF1 CC5.1-POF2 CC5.1-POF3 CC5.1-POF4 CC5.1-POF5 CC5.1-POF6			5.1	6.12						II.4.a	2	164.306(a)(1) 164.306(b)(1)		7123(b)(3)																	
				Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5		CC5.1				6.12							2	164.306(a)(1)																			
				Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5		CC5.1				6.12							2	164.306(a)(1) 164.306(d)(3)(ii)(A) 164.308(a)(1)(ii)(B)																			
				Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are:(1) Implemented correctly; and(2) Operating as intended.	5		CC4.2-POF1				6.12							2	164.306(a)(1)																			
				Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	5						6.12							2	164.306(a)(1)																			
				Intersects With	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications, Services and/or Data (TAASD) under their control on an ongoing basis for applicable threats and risks, as well as to ensure security, compliance and resilience controls are operating as intended.	5						6.12							2	164.306(a)(1)																			
				Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5		CC6.1 CC6.1-POF3 CC6.1-POF7 CC6.1-POF8 CC6.1-POF9 CC6.6 CC6.6-POF2 CC6.6-POF3		8.2.2			PR.AC-P1	AC-1 IA-1	AC-1	PR.AA PR.AA-05				164.308(a)(3)(i) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.310(a)(2)(iii) 164.312(a)(1) 164.530(c)(2)(ii)	45.48.510	7123(c)(1) 7123(c)(3) 7123(c)(3)(C)										2447(b)(5) 2447(c)(1)(A)(iv) 2447(c)(1)(B)							
				Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		CC7.2 CC7.2-POF1					CT.DM-P8	AU-1 PM-31 SI-4	AU-1 PM-31	DE.AE DE.CM-01 DE.CM-03 DE.CM-06 DE.CM-09 PR.PS-04				164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.312(b)		7123(c)(7)										2447(b)(2)(C) 2447(b)(8) 2447(b)(8)(A)							
				Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5		CC7.2 CC7.2-POF1 CC7.3						AU-2 AU-6 IR-4(4) SI-4	AU-2	DE.AE-03 DE.AE-06						7123(c)(7)																	
				Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	5		CC6.1-POF13 P4.2-POF2	7			6.11					5	II.4.a	8			7023(d)(4) 7024(f)	6-1-1305(2)(a) 6-1-1305(4) 6-1-1308(5)	15(e)(1) 15(e)(2)		45(a) 45(b) 45(c) 45(d)		5(1)(c) 6(1)(b)	47-18-3204(a)(3)		59.1-578.A.3 59.1-579.A.1 59.1-579.B.1		24.1 25.1 25.2 32.1 32.1(a) 32.1(b) 5.1(f)	19			8(4) 8(5)	Principle 5 P5-(a) P5-(a)(i) P5-(a)(ii) P5-(a)(iii) P5-(b)	
				Intersects With	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of security, compliance and resilience controls and related processes.	5		CC5.1					GV.PO-P2	PL-9	PL-9	PR.IR						7123(c)(5)(B)	6-1-1305(4) 6-1-1308(5)																
				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		CC2.3-POF10 CC5.2 CC5.2-POF4 PI1.2 PI1.3						PL-1 SA-1 SA-4 SA-23	PL-1 SA-1 SA-4	ID.RA-09 PR.PS-06						7123(c)(14)																	
				Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results.	5		CC4.1-POF1					CT.DM-P9 CT.DM-P10	SA-11 SA-11(5) SA-11(6) SA-11(7)	SA-11	ID.IM-01 ID.IM-02 ID.RA-01 PR.PS-06						7123(c)(14)																	
		Incorporate data privacy requirements into enterprise architecture to ensure that risk is addressed so Technology Assets, Applications and/or Services (TAAS) achieve the necessary levels of trustworthiness, protection and resilience.		Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	- updated in 2026.1 release	CC6.1-POF5														7123(c)(5)(B)																	

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	AICPA TSC 2017+2022 (used for SOC 2)	APEC Privacy Framework 2015	GAPP	ISO 27701 2025	ISO 29100 2024	NIST Privacy Framework 1.0	NIST 800-53 R5	NIST 800-53B R5 (privacy)	NIST CSF 2.0	OECD Privacy Principles	US Data Privacy Framework (DPF)	US FIPPS	US HIPAA Administrative Simplification 2013	US - AK PIPA	US - CA CCPA/CPRA 2025	US - CO Colorado Privacy Act	US - IL BIPA	US - IL IPA	US - IL PIPA	US - MV CDCAA	US - OR CPA	US - TN Tennessee Information Protection Act	US - TX TX DPSA	US - VA CDPA 2023	US - VT Act 171 of 2018	EMEA EU GDPR	EMEA Saudi Arabia Personal Data Protection Law (PDPL)	APAC Australia Privacy Act	APAC Australian Privacy Principles	APAC India DPDPA 2023	APAC New Zealand Privacy Act of 2020	American Canada PIPEDA
7.1	Cybersecurity Considerations		Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	S	updated in 2026.1 release																712(b)(1)(B) 712(b)(2)(B)														
				Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity, compliance and resilience requirements for each Technology Asset, Application and/or Service (TAAS) under their control.	S		CC2.1-POF1 CC2.1-POF2 CC2.1-POF3 CC2.1-POF4 CC2.1-POF5 CC5.1 CC5.1-POF1 CC5.1-POF2 CC5.1-POF3 CC5.1-POF4 CC5.1-POF5 CC5.1-POF6			5.1	6.12						6.4.a	2	164.306(a)(1) 164.306(b)(1)		712(b)(3)														
				Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	S		CC5.1				6.12								2	164.306(a)(1)														
				Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	S		CC5.1				6.12								2	164.306(a)(1) 164.306(a)(2)(iii) 164.306(a)(1)(viii)														
				Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are (1) Implemented correctly; and(2) Operating as intended.	S		CC4.2-POF1				6.12								2	164.306(a)(1)														
				Intersects With	Authorize Technology Assets, Applications, Services and/or Cloud Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	S						6.12								2	164.306(a)(1)														
				Intersects With	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications, Services and/or data (TAASD) under their control on an ongoing basis for applicable threats and risks, as well as to ensure security, compliance and resilience controls are operating as intended.	S						6.12								2	164.306(a)(1)														
				Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	S	updated in 2026.1 release	CC2.2-POF10 CC3.4 CC3.4-POF4 CC3.4-POF5 CC8.1 CC8.1-POF1 CC8.1-POF10 CC8.1-POF11 CC8.1-POF12 CC8.1-POF13 CC8.1-POF14 CC8.1-POF2 CC8.1-POF3 CC8.1-POF4 CC8.1-POF5 CC8.1-POF6 CC8.1-POF7 CC8.1-POF8 CC8.1-POF9						PR.PO-P2	CM-3 SA-8(33.a)		ID.RA-07										712(b)(4)(C) 712(b)(5)(B) 712(c)(5)(B)														
				Intersects With	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	S		CC3.4 CC3.4-POF4 CC8.1-POF10 CC8.1-POF2		1.2.6					CM-4	CM-4	ID.RA-07																				
				Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	S	updated in 2026.1 release	CC6.1-POF2 CC6.1-POF4 CC6.4 CC6.6-POF2 CC6.6-POF3								IA-4 IA-4(6)		PR.AA- PR.AA-01 PR.AA-06 PR.AA-05																	
				Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services (TSAS); and (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	S	updated in 2026.1 release	CC6.6-POF3								IA-2(1) IA-2(2)																	
				Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	S	updated in 2026.1 release	CC5.2-POF3 CC6.1 CC6.1-POF10 CC6.1-POF18 CC6.3 CC6.3-POF3								AC-2(7)		PR.AA-05																	
				Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	S	updated in 2026.1 release	CC6.1																										
				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.	S	updated in 2026.1 release	CC5.2-POF3 CC6.1 CC6.1-POF12 CC6.1-POF17 CC6.1-POF7						PR.AC-P4	AC-6 SA-8(14)		PR.AA-05 PR.DS-10							164.308(a)(3)(i) 164.312(a)(1)		712(b)(3)(iii) 712(b)(3)(iv)(A)(ii) 712(b)(3)(iii)														
				Intersects With	Management Approval for New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	S	updated in 2026.1 release	CC6.2-POF1 CC6.3-POF1								AC-2(e) IA-12(1)								164.308(a)(3)(ii)(A)		712(b)(3)(iii)														
				Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	S		CC6.1-POF13 P4.2-POF2	7			6.11						5	6.4.a	8							702.3(d)(4) 702e(f)	6-1-1305(2)(a) 6-1-1305(4) 6-1-1308(5)	15(m)(1) 15(m)(2)		45(a) 45(b) 45(c) 45(d)		5(1)(c) 8(1)(b)		47-18-3204(a)(3)		59-1-578.A.2 59-1-578.A.3 59-1-578.B.1		24.1 25.1 25.2 32.1 32.1(a) 32.1(b) 5.1(f)		19			(b)(6) 8(5)		Principle 5 Principle 7 PP-(a)(i) PP-(a)(ii) PP-(a)(iii) PP-(b)	
				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).	S		CC2.2 CC3.2 CC5.2 CC6.1-POF2 CC6.1-POF3 CC8.1-POF16		4.2.3 4.2.4 7.2.2 7.2.3				ID.IM-P6 GV.PO-P2 PR.PS-P1 CT.DM-P7 CT.DM-P8 CM.AW-P3	PT-1 SA-8 SC-1 SC-7(18) SI-1 SA-15(3)	PT-1 SI-1	PR.IR- PR.IR-01 PR.IR-03							164.306(b)(1)		712(b)(5)(B)	6-1-1305(4) 6-1-1308(5)						521.052		59-1-578.A.2 59-1-578.A.3 59-1-578.B.1		2447(a) 2447(a)(1) 2447(a)(1)(A) 2447(a)(1)(B) 2447(a)(1)(C) 2447(a)(2) 2447(a)(3)			APP Part 8 APP Part 11					Principle 7
				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.	S		CC3.1 CC6.1 CC6.1-POF2						GV.PO-P2	PL-8 PM-7	PL-8	PR.IR- PR.IR-01 PR.IR-03							164.306(b)(1) 164.308(b)(2)(iii)		712(b)(5)(B)	6-1-1305(4) 6-1-1308(5)						521.052		2447(a) 2447(a)(1) 2447(a)(1)(A) 2447(a)(1)(B) 2447(a)(1)(C) 2447(a)(2) 2447(a)(3)(D) 2447(a)(3)			APP Part 8 APP Part 11					Principle 7
				Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resilience capabilities; (3) Reduce risk exposure; and (4) Ensure conformity with applicable statutory, regulatory and/or contractual obligations.	S	updated in 2026.1 release	PI1.1-POF1 PI1.1-POF2 PI1.1-POF3							SA-23		GV.SC-09 PR.PS-06										712(b)(1)(A) 712(b)(1)(B)														
				Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	S	updated in 2026.1 release						CT.DM-P8 CT.DM-P10	SA-4(3) SA-3(1)													712(b)(1)(A)														
				Intersects With	Pre-Established Secure Configurations	TDA-02.4	Mechanisms exist to ensure vendors / manufacturer(s) to deliver the Technology Asset, Application and/or Service (TAAS) with a pre-established, secure configuration that is consistent with industry-accepted system hardening and configuration as the default for any subsequent TAAS reinstallation or upgrade.	S	updated in 2026.1 release							SA-4(5)													712(b)(1)(A)														
				Intersects With	Insecure Ports, Protocols & Services	TDA-02.6	Mechanisms exist to mitigate the risk associated with the use of insecure ports, protocols and services necessary to operate technology solutions.	S	updated in 2026.1 release																			712(b)(1)(A)														
				Intersects With	Security Compliance & Resilience Requirements For Product Changes	TDA-02.7	Mechanisms exist to include appropriate security, compliance and resilience representatives in the product feature and/or functionality change control review process.	S	updated in 2026.1 release							SA-1(b.7)													712(b)(1)(A)														
				Intersects With	Minimizing Attack Surface	TDA-02.8	Mechanisms exist to minimize the attack surface of Technology Assets, Applications and/or Services (TAAS) by reasonably mitigating known exploitable vulnerabilities.	S	updated in 2026.1 release																			712(b)(1)(A)														
				Intersects With	Ongoing Product Security Support	TDA-02.9	Mechanisms exist to deliver security updates to Technology Assets, Applications and/or Services (TAAS), where applicable, through (1) Automatic updates; and/or (2) Notification of available updates to affected users.	S	updated in 2026.1 release																			712(b)(1)(A)														
				Intersects With	Product Testing & Reviews	TDA-02.10	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for an appropriate level of security and resiliency based on applicable risks and threats.	S	updated in 2026.1 release																			712(b)(1)(A)														
				Intersects With	Disclosure of Vulnerabilities	TDA-02.11	Mechanisms exist to disclose information about vulnerabilities to relevant stakeholders that includes: (1) Affected Technology Assets, Applications and/or Services (TAAS) and versions; (2) Potential impact of the vulnerabilities; (3) Severity of the vulnerabilities; and (4) Guidance to remediate the vulnerabilities.	S	updated in 2026.1 release																			712(b)(1)(A) 712(b)(3)(i)														
				Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	S	updated in 2026.1 release	PI1.1 PI1.2 PI1.2-POF1 PI1.2-POF2 PI1.2-POF3 PI1.3 PI1.3-POF1 PI1.3-POF2 PI1.3-POF3 PI1.3-POF4 PI1.3-POF5 PI1.4 PI1.4-POF1 PI1.4-POF2 PI1.4-POF3 PI1.4-POF4 PI1.5 PI1.5-POF1 PI1.5-POF2 PI1.5-POF3 PI1.5-POF4						CT.PO-P1 CT.DM-P7 CT.DM-P8 CT.DM-P10	SA-1 SA-4(3) SA-15	SA-1	PR.PS-06													712(b)(1)(A)														
				Intersects With	Software Design Review	TDA-06.5	Mechanisms exist to have an independent review of the software design to validate (1) Applicable security, compliance and resilience requirements are met; and(2) Identified risks are remediated.	S	updated in 2026.1 release																			712(b)(1)(A)														
				Intersects With	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Technology Assets, Applications and/or Services (TAAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	S	updated in 2026.1 release																			712(b)(1)(A)														
7.2	Cryptographic Protections	Ensure personal data is encrypted both at rest and in transit.	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.	S		CC6.1 CC6.1-POF10 CC6.1-POF11 CC6.6-POF2 CC6.6-POF3 CC6.7-POF2						PR.DS-P1 PR.DS-P2	SC-8(1) SC-8(3) SC-12 SI-7(6)		PR.DS-01 PR.DS-02 PR.DS-10							164.312(e)(2)(ii) 164.312(e)(2)(iii)		712(b)(2)						2447(a)(3) 2447(b)(3)	32.1(a)							
				Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	S		CC6.1 CC6.1-POF10 CC6.7 CC6.7-POF2		6.2.1				PR.DS-P2	SC-8 SC-8(1)		PR.DS-02							164.312(e)(1)		712(b)(2)						2447(a)(3)								
				Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	S		CC6.1 CC6.1-POF10 CC6.7 CC6.7-POF2 CC6.8-POF3						PR.DS-P1	SC-12 SC-28 SC-28(1)		PR.DS-01									712(b)(2)								2447(c)(5)								
7.3	Physical Protections	Ensure physical security and environmental controls provide appropriate protection for environments where personal data is stored, transmitted and/or processed.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	S		A1.2 A1.2-POF1 A1.2-POF2 A1.2-POF3 A1.2-POF4 A1.2-POF5 A1.2-POF6 A1.2-POF7 CC6.4 CC6.4-POF1 CC6.4-POF2		8.2.3 8.2.4				PR.AC-P2 PR.PO-P4	PE-1 PE-23		DE.CM-02 ID.AM- PR.AA-06 PR.AA-08 PR.IR-02							164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iv)		712(b)(c)(5)(i)						2447(b)(7)								
				Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	S	updated in 2026.1 release	CC6.4 CC6.4-POF1 CC6.4-POF2							PE-2		PR.AA- PR.AA-06							164.310(a)(2)(ii) 164.310(a)(2)(iii)		712(b)(c)(5)(i)														
				Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	S	updated in 2026.1 release	CC6.4 CC6.4-POF1 CC6.4-POF2							PE-2(1)		PR.AA-06							164.310(a)(2)(iii)		712(b)(c)(5)(i)														
				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).	S	updated in 2026.1 release	CC6.4 CC6.4-POF1 CC6.4-POF2						PR.AC-P2	PE-3 PE-3(2) PE-3(3)		DE.CM-02 PR.AA- PR.AA-06							164.310(a)(2)(iii) 164.310(a)(2)(iii) 164.310(c)		712(b)(c)(5)(i)						2447(b)(7)								
				Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	S	updated in 2026.1 release							PR.AC-P2										164.310(b) 164.310(c)		712(b)(c)(5)(i)						2447(b)(7)								
				Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	S	updated in 2026.1 release	CC6.4-POF4							PE-6		DE.CM-02								712(b)(c)(5)(i)														
				Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	S	updated in 2026.1 release							PR.AC-P2										164.310(a)(2)(iii)		712(b)(c)(5)(i)														
7.4	Embedded Protections	Facilitate the secure implementation of embedded technologies so sensors minimize the collection of personal data and alert data subjects to the personal data collected by those sensors.	Functional	Intersects With	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	S																																	
				Intersects With	Authorized Use	END-13.1	Mechanisms exist to utilize organization-defined measures so that data or information collected by sensors is only used for authorized purposes.	S									SC-42(2)																									

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	AICPA TSC 2017+2022 (used for SOC 2)	APEC Privacy Framework 2015	GAPP	ISO 27701 2025	ISO 29100 2024	NIST Privacy Framework 1.0	NIST 800-53 R5	NIST 800-53B R5 (privacy)	NIST CSF 2.0	OECD Privacy Principles	US Data Privacy Framework (DPF)	US FIPPS	US HIPAA Administrative Simplification 2013	US - AK PIPA	US - CA CCPA 2025	US - CO Colorado Privacy Act	US - IL BIPA	US - IL IPA	US - IL PIPA	US - NV CB220	US - OR CPA	US - TN Tennessee Information Protection Act	US - TX SCUDA	US - VA CDPA 2023	US - VT Act 171 of 2018	EMEA EU GDPR	EMEA Saudi Arabia Personal Data Protection Law (PDPL)	APAC Australia Privacy Act	APAC Australian Privacy Principles	APAC India DPDPA 2023	APAC New Zealand Privacy Act of 2020	Americas Canada PIPEDA
				Intersects With	Notice of Collection	END-13.2	Mechanisms exist to notify individuals that Personal Data (PD) is collected by TAAS.	S								SC-42(4)																						
				Intersects With	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.	S								PM-25 SA-8(33) SC-42(5)	PM-25 SA-8(33)								6-1-1308(3)												
7.5	Retire Outdated Systems	Upgrade, replace, or retire any system, application or service for which appropriate protections, commensurate with risk, cannot be effectively implemented.	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.	S								SA-22																						
7.6	Personnel Security	Implement personnel management practices, covering employees, contractors and third-party users, to ensure adequate cybersecurity & data privacy for Technology Assets, Applications and/or Services (TAAS) that contain, store or transmit personal data.	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	S							GV.AT-P1 GV.AT-P2 GV.AT-P3 GV.AT-P4	AT-1 PM-13	AT-1 AT-1	PR.AT				164.308(a)(5)(i)		7123(c)(12)						2447b(2)(A) 2447b(3)(B)								
7.7	Rules of Behavior	Require employees and contractors to read and agree to abide by the organization's rules of behavior, prior to being granted access to Technology Assets, Applications and/or Services (TAAS) that store, transmit or process personal data, including social media.	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.	S								PL-4	PL-4	ID.AM				164.310(b)		7123(c)						2447b(2)(B)								
				Intersects With	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain social media restrictions and/or the use of social media and networking sites, posting information on commercial websites and sharing account information.	S								PL-4(1)	PL-4(1)																					
7.8	Employee Sanctions	Utilize employee sanctions to hold personnel accountable for complying with the organization's data privacy policies and processes.	Functional	Intersects With	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	S								PS-8						164.308(a)(1)(ii)(C) 164.530(e)(1)								2447b(4)								
7.9	Workforce Management	Respond to changing mission requirements and maintain workforce skills in a rapidly-developing technology environment through recruiting and retaining the talent needed to support the organization's mission.	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	S		CC1.1 CC1.2-POF01 CC1.3-POF02 CC1.3-POF03 CC1.3-POF04 CC1.3-POF05 CC1.3-POF06 CC2.2-POF01 CC2.2-POF02 CC2.2-POF03 CC2.2-POF04 CC2.2-POF05 CC2.3-POF01 CC2.3-POF02 CC2.3-POF03 CC2.3-POF04 CC2.3-POF05			7.2		PR.PO-P9	PS-1		GV.RR-04 ID.AM		III.9.b.ii	2	164.308(a)(3)(i)(A) 164.312(d) 164.530(e)(2)																25(i)(3)(b) 25(i)(5)(c) 25(i)(6)(c) 25(i)(7)(d) 25(i)(8)(c) 25(j) 27(1) 27(2) 27(3)	
7.10	Professional Competency	Develop and enforce data privacy competency requirements for staff members involved in the acquisition, management, maintenance and use of information resources, to ensure they have the appropriate knowledge and skill.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	S		CC1.4-POF01						PS-3						164.312(d)																
7.11	Cybersecurity & Data Privacy Control Validation	Develop and enforce an Information Assurance (IA) capability that provides a mechanism to perform pre-production control testing to ensure applicable cybersecurity & data privacy controls exist and are functioning. Systems, applications and services can also undergo Certification & Accreditation activities for authorization, following the results of pre-production control testing.	Functional	Intersects With	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	S		CC4.1 CC4.1-POF8 CC4.1-POF2 CC4.1-POF9						CA-1 PM-10	CA-1	ID.RA-01						7123(c)(4)(C)																
				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.	S		CC4.1-POF9						CA-6	CA-6							7123(c)(4)(C)																
				Intersects With	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.	S								CA-7(4)	CA-7(4)																					
				Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results.	S		CC4.1-POF1				CT.DM-P8 CT.DM-P10	SA-11 SA-11(3) SA-11(5) SA-11(7)	SA-11	ID.IM-01 ID.IM-02 ID.IM-04 PR.PS-06					7123(c)(14)																
7.12	Secure Configuration Management	Implement secure configuration management throughout the System Development Life Cycle (SDLC) to ensure Technology Assets, Applications and/or Services (TAAS) are configured according to industry-recognized secure practices.	Functional	Intersects With	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	S		CC7.1 CC7.1-POF1 CC8.1-POF12 CC8.1-POF8						PR.PO-P1	CM-1 CM-9	CM-1	PR.PS- PR.PS-01 PR.PS-05				164.308(a)(1)(i)		7123(b)(ii)(1) 7123(c)(4)(B) 7123(c)(5)	6-1-1305(4)															
				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.	S		CC6.1-POF7 CC7.1 CC7.1-POF1 CC8.1 CC8.1-POF12 CC8.1-POF6	updated in 2026.1 release					PR.PO-P1	AU-2 CM-2 CM-6 CM-7 SA-8 SA-15(5)		PR.DS-10 PR.PS- PR.PS-01				164.312(a)(2)(iii) 164.312(e)(1) 164.312(e)(2)(i) 164.312(e)(2)(ii)		7123(b)(ii)(1) 7123(c)(4)(B) 7123(c)(5) 7123(c)(5)(A) 7123(c)(5)(B)	6-1-1305(4)															
				Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results.	S		CC4.1-POF1				CT.DM-P8 CT.DM-P10	SA-11 SA-11(3) SA-11(5) SA-11(7)	SA-11	ID.IM-01 ID.IM-02 ID.IM-04 PR.PS-06					7123(c)(14)																
7.13	Situational Awareness	Correlate logs from across the organization with a Security Incident Event Manager (SIEM), or similar automated tool, to maintain situational awareness of events for potential cybersecurity & data privacy incidents.	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.	S		CC7.2 CC7.2-POF1 CC7.3							AU-2 AU-6 IR-4(4) SI-4	AU-2	DE.AE-03 DE.AE-06						7123(c)(7)														
				Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	S		CC7.2 CC7.3							AU-6(1) AU-6(3) IR-4(4) SI-4(16)		DE.AE-03 DE.AE-06																				
8	Incident Response	Maintain and test incident response plans, capabilities and training for employees and third-party stakeholders on how to report and respond to incidents.	Functional	Intersects With	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	S		A1.2-POF5 CC2.2-POF10 CC2.2-POF3 CC7.4 CC7.4-POF1 CC7.4-POF10 CC7.4-POF11 CC7.4-POF12 CC7.4-POF13 CC7.4-POF2 CC7.4-POF3 CC7.4-POF4 CC7.4-POF5 CC7.4-POF6 CC7.4-POF7 CC7.4-POF8 CC7.4-POF9			1.2.7					IR-1	IR-1	DE.AE GV.SC-08 RS RS.MI				164.308(a)(1)(ii) 164.308(a)(6)(i) 164.308(a)(7)(i)		7123(c)(17) 7123(c)(17)(B)						2447b(1)(E) 2447b(3)(E)(ii)(A)								
				Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	S		A1.2-POF5 CC2.2-POF10 CC2.2-POF3 CC2.2-POF6 CC2.2-POF8 CC7.4 CC7.4-POF1 CC7.4-POF10 CC7.4-POF11 CC7.4-POF12 CC7.4-POF13 CC7.4-POF2 CC7.4-POF3 CC7.4-POF4 CC7.4-POF5 CC7.4-POF6 CC7.4-POF7 CC7.4-POF8 CC7.4-POF9			1.2.7			GV.WT-P4 GV.WT-P5	IR-4	IR-4	DE.AE DE.AE-02 DE.AE-03 DE.AE-04 DE.AE-06 DE.AE-07 GV.SC-08 RC.RP-06 RS RS.AN RS.AN-03 RS.CO RS.CO-02 RS.CO-03 RS.MA RS.MA-01 RS.MA-02 RS.MA-04 RS.MI RS.MI-01 RS.MI-02				164.308(a)(6)(ii) 164.412 164.412(a) 164.412(b) 164.530(f)		7027(m)(2) 7123(c)(17)(A)						2447b(1)(E) 2447b(3)(E)(ii)(A)								
				Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	S		CC2.2-POF10 CC2.2-POF8 CC7.3 CC7.3-POF1 CC7.4 CC7.4-POF1 CC7.4-POF10 CC7.4-POF11 CC7.4-POF12 CC7.4-POF13 CC7.4-POF2 CC7.4-POF3 CC7.4-POF4 CC7.4-POF5 CC7.4-POF6 CC7.4-POF7 CC7.4-POF8 CC7.4-POF9			1.2.7			PR.PO-P7	IR-8	IR-8	DE.AE-08 ID.IM-04 RC RS.MA RS.MA-01 RS.MA-02 RS.MA-04 RS.MI								7123(c)(17)(B)(i)						2447b(1)(E) 2447b(3)(E)(ii)(A)								
				Intersects With	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	S		CC7.3 CC7.3-POF04 PL-2 PM-9 PM-9-POF02 RA-3			1.2.7 7.2.4			GV.WT-P4 GV.WT-P5	IR-8(1)	IR-8(1)					164.404(a)(1) 164.404(a)(2) 164.404(c)(1)(A) 164.404(c)(1)(B) 164.404(c)(1)(C) 164.404(c)(2) 164.406(1)(2) 164.408(1)(2) 164.408(a) 164.408(b) 164.408(c) 164.410(c)(1)				10(a) 10(a)(1)(A) 10(a)(1)(B) 10(a)(1)(C) 10(a)(2) 10(b) 10(c)(1) 10(c)(2) 10(c)(3) 10(d) 10(e)(1) 10(e)(2) 10(e)(2)(A) 10(e)(2)(B) 10(e)(2)(C)				521.053				33.1	28.1 28.2			8(4)		
				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.	S								PR.PO-P8	IR-3 IR-3(2)	IR-3							7123(c)(17)(B)(ii)												
				Intersects With	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.	S					1.2.7				IR-7	IR-7																			
8.1	Coordinated Response	Respond to incidents in a coordinated and structed manner to ensure the appropriate steps are taken to identify and respond to potential incidents.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	S		A1.2-POF5 CC2.2-POF10 CC2.2-POF3 CC2.2-POF6 CC2.2-POF8 CC7.3 CC7.3-POF1 CC7.3-POF2 CC7.3-POF3 CC7.3-POF4 CC7.3-POF5 CC7.3-POF6 CC7.3-POF7 CC7.4 CC7.4-POF1 CC7.4-POF10 CC7.4-POF11 CC7.4-POF12 CC7.4-POF13 CC7.4-POF2 CC7.4-POF3 CC7.4-POF4 CC7.4-POF5 CC7.4-POF6 CC7.4-POF7 CC7.4-POF8 CC7.4-POF9			1.2.7			GV.WT-P4 GV.WT-P5	IR-4	IR-4	DE.AE DE.AE-02 DE.AE-03 DE.AE-04 DE.AE-06 DE.AE-08 GV.SC-08 RC.RP-06 RS RS.AN RS.AN-03 RS.CO RS.CO-02 RS.CO-03 RS.MA RS.MA-01 RS.MA-02 RS.MA-04 RS.MI RS.MI-01 RS.MI-02				164.308(a)(6)(ii) 164.412 164.412(a) 164.412(b) 164.530(f)		7027(m)(2) 7123(c)(17)(B)(i)						2447b(1)(E) 2447b(3)(E)(ii)(A)								
				Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	S									IR-4(11)		DE.AE-06 RS RS.MA RS.MA-01 RS.MA-04								521.053								

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	AICPA TSC 2017+2022 (used for SOC 2)	APEC Privacy Framework 2015	GAPP	ISO 27701 2025	ISO 29100 2024	NIST Privacy Framework 1.0	NIST 800-53 R5	NIST 800-53B R5 (privacy)	NIST CSF 2.0	DSCD Privacy Principles	US Data Privacy Framework (DPF)	US FCPD	US HIPAA Administrative Simplification 2013	US - AK PIPA	US - CA CCPA 2025	US - CO Colorado Privacy Act	US - IL BIPA	US - IL IDTA	US - IL PIPA	US - NV CB220	US - OR CPA	US - TN Tennessee Information Protection Act	US - TX SCI21	US - VA CDPA 2023	US - VT Act 171 of 2018	EMEA EU GDPR	EMEA Saudi Arabia Personal Data Protection Law (PDPL)	APAC Australia Privacy Act	APAC Australian Privacy Principles	APAC India DPDPA 2023	APAC New Zealand Privacy Act of 2020	Americas Canada PIPEDA
8.2	Breach Notification	Report data breaches involving personal data to relevant regulators, law enforcement and affected parties in accordance with applicable statutory, regulatory and contractual obligations for breach notification.	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.	S		CC2.3-POF6 CC3.2 CC7.3-POF1 CC7.3-POF8 CC7.3-POF2 CC7.4 CC7.4-POF13 CC7.4-POF6 CC7.4-POF8 CC7.5-POF2 P6.2 P6.7		1.2.7		6.10		IR-6	IR-6	DE.AE-06 RS.AN-03 RS.CO-02 RS.CO-03 RS.MA-01				164.404(b) 164.408(a) 164.408(b) 164.408(c)						521.053			34.1 34.2					8(6)		
				Intersects With	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	S		CC2.3-POF6 CC2.3-POF12 CC2.3-POF2 CC7.4						IR-7(2)																								
9	Risk Management	Implement a risk management framework to ensure that risks are identified, evaluated and addressed to achieve necessary levels of trustworthiness, protection and resilience.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	S		A1.2-POF1 CC3.1 CC3.1-POF1 CC3.2-POF2 CC3.3-POF1 CC3.4-POF1 CC3.4-POF2 CC3.4-POF3 CC3.4-POF4 CC3.4-POF5 CC5.1 CC5.1-POF1 CC9.1				6.1.2	ID.GV-P1 GV.RM-P1	PM-9 PM-28 RA-1	RA-1	GV GV.OV-02 GV.OV-03 GV.RM GV.RM-01 GV.RM-03 GV.RM-04 GV.RM-06 GV.SC GV.SC-01 GV.SC-02 GV.SC-03 GV.SC-06 ID ID.IM PR PR.IR				164.306(a)(3) 164.306(b)(2)(iv)										24470(b)(2)	32.2						
					Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	S	updated in 2026.1 release	CC9.1-POF1 CC9.1-POF2				6.1.3				GV.RM-04 GV.RA-05				164.306(d)(3)(ii)(B) (2)			7002(d)(3)														
					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 cybersecurity & data privacy compliance and resilience controls, compliance and change management.	S									CA-7(4)	CA-7(4)																					
9.1	Evaluate Risks	Utilize appropriate risk analysis methods to evaluate the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of personal data where it is stored, transmitted and/or processed.	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).	S		A1.2 CC3.1-POF16 CC3.2 CC3.2-POF2 CC3.2-POF3 CC3.2-POF4 CC3.2-POF6 CC3.2-POF9 CC3.3 CC3.4 CC3.4-POF2 CC3.4-POF3 CC3.4-POF5 CC7.3		1.2.4	6.1.2(e)		ID.DE-P1 ID.GV-P1 GV.MT-P1	RA-3	RA-3	GV.RM-04 ID ID.RA-01 ID.RA-03				164.306(b)(2)(iv) 164.308(a)(1)(ii)(A)			7152(a) 7155(a)																	
				Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	S	updated in 2026.1 release																7155(a) 7155(b) 7155(b)(1) 7155(b)(2) 7155(b)(2)(A) 7155(b)(3) 7155(b)(4) 7155(b)(5) 7155(b)(6) 7155(b)(7) 7155(d)(2 7155(d)(3) 7155(d) 7155(e)															
				Intersects With	Risk Assessment Stakeholder Involvement	RSK-04.4	Mechanisms exist to: (1) Define applicable stakeholders for each risk assessment process; (2) Identify applicable stakeholders for each risk assessment process; and (3) Provide identified stakeholders with results of the risk assessment, upon completion.	S	updated in 2026.1 release																7151(e) 7151(b)											
9.2	Assess Supply Chain Risk	Assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS) for data privacy implications.	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	S		CC3.2 CC3.2 CC9.1-POF1 CC9.1-POF2																														
				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.	S		CC3.1 CC3.2 CC3.2-POF7 CC3.2-POF8 CC6.2 CC9.2-POF1 CC9.2-POF10 CC9.2-POF11 CC9.2-POF12 CC9.2-POF2 CC9.2-POF3 CC9.2-POF4 CC9.2-POF7 CC9.2-POF8 CC9.2-POF9					ID.DE-P1 ID.GV-P1	PM-26 PM-30 SA-9(3) SR-3 SR-7		GV.SC GV.SC-01 GV.SC-03 GV.SC-05 GV.SC-06 GV.SC-10 ID ID.IM PR PR.PS																						
				Intersects With	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	S		CC3.2-POF7 CC3.2-POF9 CC6.1 CC9.2-POF1 CC9.2-POF11 CC9.2-POF12 CC9.2-POF2 CC9.2-POF7					ID.DE-P1 GV.MT-P1	RA-3(1)		GV.SC GV.SC-09																		
9.3	Risk Awareness	Maintain a current and accurate register of risk (e.g., Plan of Action & Milestones (POA&M), risk register, etc.).	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Control deficiency/gap; (2) Impact to the organization's cybersecurity and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/discovery; and (6) Status of planned remediation, if applicable.	S		CC4.2 CC9.2-POF3						CA-5 SA-5(a,c)	CA-5	ID.IM-01 ID.IM-02 ID.RA-01																		
				Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	S		CC4.2-POF2					ID.DE-P1			GV.RM-04 ID ID.RA-01																		
				Intersects With	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.	S									CA-7(4)	CA-7(4)																		
9.4	Risk Response	Respond to identified risks are appropriately identified, categorized and prioritized.	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related (1) Assessments; (2) Audits; and/or (3) Incidents.	S		CC3.3-POF5				6.1.3		ID.DE-P1 ID.RA-P5	RA-7	RA-7	GV.RM-04 ID.RA-01 ID.RA-06																					
9.5	Data Protection Impact Assessment (DPIA)	Utilize Data Protection Impact Assessments (DPIAs) to effectively identify and reduce data privacy risks to an acceptable level.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	S		CC3.2 CC3.2 P3.1.2		1.2.4 4.2.3	6.1.2 6.1.2(a) 6.1.2(a)(2) 6.1.2(b) 6.1.2(c) 6.1.2(c)(1) 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.2		ID.DE-P1 ID.GV-P2 ID.GV-P3 ID.RA-P4 ID.RA-P5 ID.DE-P2 ID.DE-P3 GV.MT-P3 GV.MT-P4 GV.MT-P5	RA-8	RA-8					7154(a) 7153(a)(1) 7153(a)(2) 7153(a)(3) 7152(a)(2)(A) 7152(a)(2)(B) 7152(a)(2)(C) 7152(a)(2)(D) 7152(a)(2)(E) 7152(a)(2)(F) 7152(a)(2)(G) 7152(a)(2)(G)(i) 7152(a)(2)(G)(ii) 7153(a)(4) 7152(a)(5) 7152(a)(5)(A) 7152(a)(5)(B) 7152(a)(5)(C) 7152(a)(5)(D) 7152(a)(5)(E) 7152(a)(5) 7152(a)(5)(F) 7152(a)(5)(G) 7152(a)(5)(H) 7152(a)(6) 7152(a)(6)(A) 7152(a)(6)(A)(i) 7152(a)(6)(A)(ii) 7152(a)(6)(A)(iii) 7152(a)(6)(B) 7153(a)(7) 7153(a)(8) 7153(b) 7155(a) 7155(b)	6-1-1305(2)(c) 6-1-1306(1) 6-1-1308(1) 6-1-1308(2) 6-1-1309(2)(a)(I) 6-1-1309(2)(a)(II) 6-1-1309(2)(a)(III) 6-1-1309(2)(a)(IV) 6-1-1309(2)(b) 6-1-1309(2)(c) 6-1-1309(3) 6-1-1309(4) 6-1-1309(5) 6-1-1309(6)					61(3)(c) 61(3)(d) 8(2)(b)	47-18-3206(a) 47-18-3206(a)(1) 47-18-3206(a)(2) 47-18-3206(a)(3) 47-18-3206(a)(4)(A) 47-18-3206(a)(4)(B) 47-18-3206(a)(4)(C) 47-18-3206(a)(4)(D) 47-18-3206(a)(5) 47-18-3206(b) 47-18-3206(c) 47-18-3206(d) 47-18-3206(e) 47-18-3206(f)		58.1-580.A 58.1-580.A.1 58.1-580.A.2 58.1-580.A.3 58.1-580.A.4 58.1-580.B 58.1-580.C 58.1-580.D 58.1-580.E 58.1-580.F 58.1-580.G		35.1 35.11 35.2(a) 35.2(b) 35.2(c) 35.7(b) 35.7(c) 35.8 35.8 36.1		22		10(2)(c)(ii)		
10	Third-Party Management	Provide data privacy oversight of third-parties with access to personal data, so that only trusted third-parties are contracted with.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	S		CC1.1-POF1 CC1.4-POF2 CC1.4-POF3 CC2.2-POF11 CC2.2-POF12 CC2.3-POF9 CC3.4 CC3.4-POF5 CC9.1 CC9.2 CC9.2-POF1 CC9.2-POF10 CC9.2-POF11 CC9.2-POF12 CC9.2-POF2 CC9.2-POF3 CC9.2-POF4 CC9.2-POF5 CC9.2-POF6 CC9.2-POF8 CC9.2-POF9				6.1.3(h)		GV.PO-P6	SR-6 SR-1	SA-4	GV.SC-04 GV.SC-06 GV.SC-07 GV.SC-08 GV.SC-10 ID.AM				164.308(b)(1) 164.312(d)			7024(f) 7052(a) 7123(c)(5)(I)		6-1-1305(6) 6-1-1305(7)									24470(d) 24470(d)(A) 24470(d)(B)						
				Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	S		CC3.3						SA-9	SA-9	GV.SC-06 GV.SC-07				164.308(b)(1)			7122(c)(1)(I)													
				Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	S	updated in 2026.1 release	CC1.4-POF2 CC1.4-POF3 CC3.4 CC3.4-POF1 CC4.1 CC9.2-POF12 CC9.2-POF13 CC9.2-POF2 CC9.2-POF3 CC9.2-POF8						SR-6 SR-6(1)		GV.SC-07 ID.IM-01 ID.IM-02								7051(c) 7052(b) 7123(c)(1)(I)			24470(d) 24470(d)(A) 24470(d)(B)		6				
				Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	S	updated in 2026.1 release	CC4.2 CC4.2-POF8 P6.4-POF2 P6.4-POF3 P6.5-POF2 P6.6-POF1								GV.SC-06 GV.SC-07 GV.SC-08								7053(a)(5) 7123(c)(1)(I)			24470(d) 24470(d)(A) 24470(d)(B)						
				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.	S	updated in 2026.1 release	CC3.4 CC3.4-POF1 CC4.1 CC9.2-POF10						SA-4	SA-4	GV.SC-08							7123(c)(1)(I)									
10.1	Supply Chain Protections	Govern the disclosure of personal data to ensure it is only provided to trusted third-parties that can store, process and/or transmit it in a secure manner.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to to evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains, and/or other third-party risks, and take appropriate steps to minimize the organization's exposure to those risks and threats, as necessary.	S		CC1.1-POF1 CC1.1-POF7 CC9.1 CC9.2-POF1 CC9.2-POF10 CC9.2-POF12 CC9.2-POF2 CC9.2-POF3 CC9.2-POF4 CC9.2-POF7 CC9.2-POF8 CC9.2-POF9						SA-8(3) SR-3 SR-2(1)		GV.SC GV.SC-05 GV.SC-07								7123(c)(1)(I)			24470(d) 24470(d)(A) 24470(d)(B)						
			Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	S		CC3.3						SA-9	SA-9	GV.SC-06 GV.SC-07				164.308(b)(1)			7123(c)(1)(I)													
10.2	Secure Disclosure To Third-Parties	Govern third-party use of personal data to ensure data privacy requirements are enforced when a third-party stores, processes or transmits personal data on behalf of the organization.	Functional	Intersects With	Information Sharing With Third-Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	S		P6.1 P6.1-POF1			7.2.1 7.2.2 7.2.3		6.10	CT.PO-P2	AC-21						164.506(c)(1) 164.506(c)(2) 164.506(c)(3) 164.508(a)(1) 164.508(a)(4)(i)	45.48.420 45.48.430			6-1-1305(7) 6-1-1305(8)(a) 6-1-1305(8) 6-1-1307(3) 6-1-1307(4)					8		APP 7 APP 8		8(2)		Sec 20 Sec 23

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	AICPA TSC 2017-2022 (used for SOC 2)	APEC Privacy Framework 2015	GAPP	ISO 27701 2025	ISO 29100 2024	NIST Privacy Framework 1.0	NIST 800-53 R5	NIST 800-53B R5 (privacy)	WEF CAF 2.0	GV.SC-05	OECD Privacy Principles	US Data Privacy Framework (DPF)	US FDPO	US HIPAA Administrative Simplification 2013	US - AK PIPA	US - CA CCPA CPRA 2023	US - CO Colorado Privacy Act	US - IL BIPA	US - IL IPA	US - IL PIPA	US - NV SB220	US - OR CPA	US - TN Tennessee Information Protection Act	US - TX BIPA	US - TX SCUDA	US - VA CDPA 2023	US - VT Act 171 of 2018	EMEA EU GDPR	EMEA Saudi Arabia Personal Data Protection Law (PDPL)	APAC Australia Privacy Act	APAC Australian Privacy Principles	APAC India DPDPA 2023	APAC New Zealand Privacy Act of 2020	American Canada PIPEDA
10.3	Contractual Obligations for Third-Parties	Acquire terms and conditions in contracts and other agreements to cover the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of personal data.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5		P6.1-POF1 P6.4 P6.4-POF3		4.2.3 7.2.4		6.10	ID.DE-P3				GV.SC-05				164.504(e)(2)(ii) 164.504(e)(2)(ii)(A) 164.504(e)(2)(ii)(B) 164.504(e)(2)(ii)(C) 164.504(e)(3)(i)(A) 164.504(e)(3)(i)(B) 164.504(e)(4)(i)(B) (iii)(B)		7022(c) 7022(c)(1) 7022(c)(1)(7022(c)(2) 7022(c)(2)(7022(d) 702(e) 7026(a) 7050(a) 7050(a)(1) 7050(a)(2) 7050(a)(3) 7050(a)(4) 7050(a)(5) 7050(b) 7050(c) 7050(d) 7050(e) 7050(f)(1) 7050(f)(2) 7051(a) 7051(a)(1) 7051(a)(2) 7051(a)(3) 7051(a)(4) 7051(a)(5) 7051(a)(6) 7051(a)(7) 7051(a)(8) 7053(a)(1) 7053(a)(2)	6-1-1305(3)(b) 6-1-1305(5) 6-1-1305(5)(a) 6-1-1305(5)(b) 6-1-1305(5)(c) 6-1-1305(5)(d)(I) 6-1-1305(5)(d)(II)(A) 6-1-1305(5)(d)(II)(B) 6-1-1305(6) 6-1-1305(7) 6-1-1307(2) 6-1-1307(3)				45(a) 45(b)(1) 45(c) 45(d) 50			4(1) 4(1)(a) 4(2) 4(3)(a)(C)	47-18-1205(a) 47-18-1205(a)(1) 47-18-3205(a)(2) 47-18-3205(b) 47-18-3205(b)(1) 47-18-3205(b)(2) 47-18-3205(b)(3) 47-18-3205(c) 47-18-3205(d)			59.1-576.A 59.1-576.A.1 59.1-576.A.2 59.1-576.A.3 59.1-576.A.4 59.1-576.A.5 59.1-576.A.6 59.1-581.A.3 59.1-581.A		28.1 28.10 28.2 28.3 28.3(a) 28.3(b) 28.3(c) 28.3(d) 28.3(f) 28.3(g) 28.4 28.4 28.5 28.6 28.7 28.8 29 46.3(a)					APP 7		Principle 5 PS-5(a) PS-5(b) PS-5(c) PS-5(d)	Sec 20 Sec 23
				Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		CC1.3-POF5 CC2.3-POF10 CC2.3-POF2 CC2.3-POF3 CC2.3-POF5 CC2.3-POF7 CC4.1 CC4.1-POF1 CC5.2-POF10 CC9.2-POF5 CC9.2-POF6 P6.4 P6.4-POF3			6.1.3(h)			ID.DE-P3 GV.RM-P4 GV.RM-P6 GV.AT-P4	SA-3(3)		GV.OC-02 GV.OC-03 GV.SC-03 GV.SC-05 GV.SC-06		8.3.a 8.3.b 8.3.c 8.3.d A.18.a.i A.18.a.ii.1 A.18.a.ii.2 A.18.a.ii.3 A.18.a.iii		164.314(a)(2)(i) 164.314(a)(2)(i)(A) 164.314(a)(2)(i)(B) 164.314(a)(2)(i)(C) 164.502(e)(1)(i) 164.502(e)(2)(i) 164.504(e)(1)(i) 164.504(e)(2) 164.504(e)(2)(ii) 164.504(e)(2)(ii)(B) 164.504(e)(2)(ii)(C) 164.504(e)(3) 164.504(e)(3)(i) 164.504(e)(3)(i)(A) 164.504(e)(3)(i)(B) 164.504(e)(3)(i)(C) 164.504(e)(3)(ii) 164.504(e)(3)(ii)(A) 164.504(e)(3)(ii)(B) 164.504(e)(3)(iii) 164.504(e)(4)(i) 164.504(e)(4)(ii) 164.504(e)(5) 164.504(f)(1) 164.504(f)(2)(i) 164.504(f)(2)(ii) 164.504(f)(2)(iii) 164.504(f)(2)(iv) 164.504(f)(2)(v) 164.504(f)(3) 164.504(g)(1) 164.504(g)(2)		7012(a) 7052(a) 7052(b) 7053(a)(6) 7123(c)(3) 7123(c-1)(a)(3) 7123(c-1)(a)(4)(7153(a)	6-1-1305(3)(b) 6-1-1305(5) 6-1-1305(5)(a) 6-1-1305(5)(b) 6-1-1305(5)(c) 6-1-1305(5)(d)(I) 6-1-1305(5)(d)(II)(A) 6-1-1305(5)(d)(II)(B) 6-1-1305(6)				45(a) 45(b)(1) 45(c) 45(d) 50		6(2)(a) 6(2)(b) 6(2)(c) 6(2)(d) 6(2)(e) 6(2)(f) 6(2)(g) 6(2)(h)			59.1-576.A.5		24473(b)(6) 24473(b)(8)(A) 24473(b)(8)(B)	8						B(7)(b)	
10.4	Third-Party Compliance	Validate that data privacy controls for Technology Assets, Applications and/or Services (TAAS) used or operated by third-parties are effectively implemented and align with industry-recognized secure practices, as well as comply with applicable statutory, regulatory and contractual obligations.	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		P6.8 P8.1-POF6		1.2.6 10.2.1 10.2.4 10.2.5				PM-14	PM-14																											
				Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		CC3.3						SA-9	SA-9	GV.SC-06 GV.SC-07					164.308(b)(1)		7123(c)(5)																
				Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	updated in 2026.1 release	CC1.1-POF5 CC1.3-POF3 CC1.3-POF4 CC2.2-POF2 CC2.2-POF5 CC2.2-POF9 CC2.3-POF4 CC2.3-POF6 CC2.3-POF9 CC4.1-POF3 CC9.2-POF4						SA-9(3)		GV.OC GV.OC-02 GV.RM-05 GV.RR GV.SC-02 GV.SC-05 GV.SC-06 ID.AM			164.308(b)(1)		7052(a) 7123(c)(5) 7123(c-1)(a)(4)(i)														
				Intersects With	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure security, compliance and resilience control responsibilities are clearly defined for each Technology Asset, Service and/or External Service Provider (ESP) (1) Business processes; (2) Applicable stakeholders; and(4) Deployed Technology Assets, Applications and/or Services (TAAS).	5	updated in 2026.1 release	CC2.2-POF8 CC2.3-POF12 CC9.2-POF17									GV.SC-06						7123(c)(5)												
				Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	updated in 2026.1 release	CC1.4-POF2 CC1.4-POF3 CC3.4 CC3.4-POF1 CC9.1 CC9.2-POF10 CC9.2-POF12 CC9.2-POF6 CC9.2-POF7 CC9.2-POF8						SA-9 SA-9(1)		GV.SC-07 ID.IM-02 ID.IM-02					7053(a) 7053(b) 7123(c)(5)					24473(b)(6) 24473(b)(8)(A) 24473(b)(8)(B)	8						
				Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	updated in 2026.1 release	CC2.2 CC4.2 CC4.2-POF8 P6.8-POF2 P6.8-POF3 P8.1-POF1 P8.1-POF4									GV.SC-08 GV.SC-07 GV.SC-08						7053(a)(5) 7123(c)(5)					24473(b)(6) 24473(b)(8)(A) 24473(b)(8)(B)							
				Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business information, systems, applications, Services and/or Data (TAASD) that are in scope by the third-party.	5	updated in 2026.1 release	CC3.4 CC3.4-POF5 CC9.1 CC9.2-POF8						SA-4	SA-4	GV.SC-08						7123(c)(5)												
11	Business Environment	The organization's mission, objectives, stakeholders and activities are understood and prioritized to provide resourcing and guidance for data privacy roles, responsibilities and risk management decisions.	Functional	Intersects With	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 (SCRP) and document all exceptions to this requirement.	5		CC1.4			7.1			PM-3		GV.RR-03																		
				Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5		CC1.1-POF5 CC1.4-POF2 CC1.4-POF3 CC2.2-POF10 CC2.3-POF9 CC3.4 CC3.4-POF5 CC9.1 CC9.2 CC9.2-POF1 CC9.2-POF10 CC9.2-POF11 CC9.2-POF12 CC9.2-POF2 CC9.2-POF3 CC9.2-POF4 CC9.2-POF5 CC9.2-POF6 CC9.2-POF7 CC9.2-POF8 CC9.2-POF9			6.1.3(h)			GV.PO-P4	SA-4 SA-1	SA-4	GV.SC-04 GV.SC-06 GV.SC-07 GV.SC-08 GV.SC-10 ID.AM			164.308(b)(1) 164.312(d)		7024(l) 7052(a) 7123(c)(5)	6-1-1305(6) 6-1-1305(7)											24473(b)(6) 24473(b)(8)(A) 24473(b)(8)(B)							
11.1	Data Privacy Protections Context	Identify and document the organization's role as a controller and/or processor of sensitive/regulated data, including instances involving more than one party.	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	5		CC3.2-POF1 CC3.2-POF10 CC3.2-POF11 CC3.2-POF3 CC3.2-POF4			4.1 6.1.1			ID.AM-P5 ID.BE-P1 GV.OC-01 GV.RM-P3			GV.OC GV.OC-01 GV.OC-04 GV.OV-01 GV.SC-02			164.306(b)(2)(i)																	
				Intersects With	Joint Processing of Personal Data (PD)	PRI-07.2	Mechanisms exist to clearly define and communicate the organization's role in processing Personal Data (PD) in the data processing ecosystem.	5								ID.BE-P1								6-1-1305(7)				6(1)(a)	47-18-3205(d)									
11.2	Policies, Standards & Procedures	Ensure appropriate policies, standards and procedures exist to operationalize the data privacy program.	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		CC1.1-POF1 CC1.4-POF1 CC2.2-POF1 CC2.2-POF7 CC3.1 CC5.3-POF1 CC7.2-POF1 P1.1-POF5			8.2.1			GV.PO-P1 GV.PO-P6 GV.MT-P2 GV.MT-P4 GV.MT-P5 GV.MT-P6 GV.MT-P7 CT.PO-P1 CT.PO-P2 CT.PO-P3 CM.PO-P1 PR.PO-P4	AC-1 AT-1 CA-1 CM-1 CP-1 IR-1 MA-1 MP-1 PE-1 PL-1 PM-1 PS-1 PT-1 RA-1 SA-1 SC-1 SI-1 SR-1		GV.PO GV.PO-01 GV.SC-01 GV.SC-02 ID.RA	45.48.530	7123(b)(1)	164.308(a)(1)(i) 164.308(a)(1)(ii) 164.308(a)(2)(i) 164.308(a)(4)(ii) 164.308(a)(4)(ii)(A) 164.308(a)(4)(ii)(B) 164.308(a)(5)(i) 164.310(a)(1) 164.310(b)(2)(iii) 164.310(d)(1) 164.310(d)(2)(i) 164.310(d)(2)(ii) 164.312(a)(1) 164.312(b) 164.316(b)(2)(ii)											24473(b)(3)	24.2			APP 1				
				Intersects With	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to: (1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role;(2) Ensure that organizational data privacy practices are publicly available and communicated through organizational document repositories;(3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy officials regarding the data privacy practices; and(4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.	5		P1.1 P1.1-POF6			2.1.1 2.2.1 2.2.2 2.2.3 2.3.1 3.1.1 4.1.0 4.1.1 4.2.4 5.1.0 5.1.1 6.1.0 6.1.1 7.1.1 8.1.0 8.1.1 9.1.0 9.1.1 10.1.1	4.2(e) 7.3 7.5.3(a)	6.8	GV.PO-P1 CM.AW-P1	PM-20	PM-20		G		II																				
11.3	Periodic Review	At planned intervals or after significant changes, review policies, standards and procedures to ensure the continuing suitability, adequacy and effectiveness to meet the organization's applicable statutory, regulatory and contractual needs.	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 when significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		CC2.2-POF7 CC3.1 CC5.3-POF6			8.2.1			GV.MT-P2	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PM-1 PS-1 PT-1 RA-1 SA-1 SC-1 SI-1 SR-1		GV.OV GV.OV-01 GV.OV-03 GV.PO-02	45.48.530		164.314(b)(2)(iii) 164.316(b)(2)(iii)											24473(b)(8)(B) 24473(b)(8)(C) 24473(b)(8)(A) 24473(b)(8)(B)							
				Intersects With	Security, Compliance & Resilience Controls Oversight	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		CC5.1-POF3 CC4.1			10.2.4			ID.DE-P5	CA-2	CA-2	ID.IM-02 ID.IM-03			164.306(d)(3)(i) 164.316(b)(2)(iii)		7120(a) 7120(b)												
11.4	Oversight	Provide oversight of data privacy controls throughout the lifecycle of Technology Assets, Applications and/or Services (TAAS) to ensure that in a timely manner, senior leaders with the organization are made aware of data privacy-related risks that are not appropriately remediated.	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		CC1.3 CC1.3-POF3 CC2.2 CC2.2-POF1 CC4.1-POF1 CC4.1-POF2 CC4.1-POF3			8.2.3 9.2.2(a) 9.2.2(b) 9.2.2(c)	6.12		GV.MT-P4 PR.PO-P5	CA-7 CA-7(1) PM-14	CA-7	GV.OC-03			164.306(d)(3)(i) 164.316(b)(2)(iii)	45.48.520	7123(a)(3) 7120(f)										24473(b)(2)(C) 24473(b)(8) 24473(b)(8)(A)	32.1(d)		APP Part 11				Principle 7	
				Intersects With	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.	5								CT.DM-P8	PM-23 PM-24	PM-24																		
				Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5		CC2.3-POF2 CC2.3-POF3 CC2.3-POF5 CC3.1-POF10 CC3.1-POF11 CC4.2 CC4.2-POF1 CC4.2-POF2			5.1 5.2(b) 9.3.1						GV.OV GV.OV-01 GV.OV-02 GV.SC-09 ID																	10(2)(c)(ii)			

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	AICPA TSC 2017-2022 (used for SOC 2)	APEC Privacy Framework 2015	GAPP	ISO 27701 2025	ISO 29100 2024	NIST Privacy Framework 1.0	NIST 800-53 R5	NIST 800-53B R5 (privacy)	NIST CSF 2.0	OECD Privacy Principles	US Data Privacy Framework (DPF)	US FIPPS	US HIPAA Administrative Simplification 2013	US - AK PIPA	US - CA CCPA 2025	US - CO Colorado Privacy Act	US - IL BIPA	US - IL IPA	US - IL PIPA	US - NV CB220	US - OR CPA	US - TN Tennessee Information Protection Act	US - TX SCUI	US - VA CDPA 2023	US - VT Act 171 of 2018	EMEA EU GDPR	EMEA Saudi Arabia Personal Data Protection Law (PDPL)	APAC Australia Privacy Act	APAC Australian Privacy Principles	APAC India DPDPA 2023	APAC New Zealand Privacy Act of 2020	Americas Canada PIPEDA
11.5	Metrics & Trends		Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5		CC1.1-POF3 CC1.2 CC1.3 CC1.5-POF2 CC1.5-POF5 CC2.1-POF4 CC2.2 CC4.1 CC4.2-POF2 CC4.2-POF3 CC5.1-POF6			9.1		GV.MT-P4 PR.PO-P5 PR.PO-P6	PM-6		GV.OV GV.OV-03 GV.SC-07 GV.SC GV.SC-09 ID.IM-02																					
				Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5		CC2.2-POF2 CC2.2-POF3 CC2.3-POF5 CC3.2-POF10 CC3.2-POF11 CC4.2 CC4.2-POF1 CC4.2-POF2			5.1 5.2(b) 9.3.1					GV.OV GV.OV-03 GV.SC-07 GV.SC GV.SC-09 ID																			30(2)(c)(ii)			
				Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5		CC1.1-POF3 CC1.2 CC1.3 CC1.5-POF2 CC1.5-POF5 CC2.1-POF4 CC2.2 CC4.1 CC4.2-POF2 CC4.2-POF1 CC5.1-POF6			9.1		GV.MT-P4 PR.PO-P5 PR.PO-P6	PM-6		GV GV.OV GV.OV-03 GV.SC-07 GV.SC GV.SC-09 ID.IM-02																					
				Intersects With	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	5		CC2.3 P8.1-POF4 P8.1-POF5			10.2.3 10.2.5			CM.AW-P4 CM.AW-P5 CM.AW-P7	PM-27	PM-27																30.1 30.1(a) 30.1(b) 30.1(c) 30.1(d) 30.1(e) 30.1(f) 30.1(g) 30.2 30.2(a) 30.2(b) 30.2(c) 30.2(d) 30.3	31 31.1 31.2 31.3 31.4 31.5 31.6 31.6								
11.6	Compliance	Oversee the execution of data privacy controls to create appropriate evidence of due diligence and due care, demonstrating compliance with all applicable statutory, regulatory and contractual obligations, including age-based restrictions.	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		CC1.5 CC2.2 CC2.3 CC3.2-POF1 CC3.2-POF14 CC5.1-POF6 CC5.1-POF8 CC9.1-POF9			4.1 4.2(a) 4.2(b) 4.3(c)	6.12	GV.PO-P5 GV.MT-P3	PL-1 PM-8	PL-1	GV.OC GV.OC-03 GV.SC-05 PR		8.7.c 8.5.a 8.5.a.i		164.306(c) 164.308(a)(1) 164.308(a)(2) 164.314(a)(1) 164.314(a)(2)(i) 164.504(g)(2)		7013(b) 7022(d) 7023(b) 7050(b) 7072(b) 7075(b) 7080(d) 7200(b)	6-1.1305(1) 6-1.1307(1) 6-1.1307(3) 6-1.1307(5) 6-1.1308(b)		45(a) 45(b) 45(d) 45(d) 50		7(1)(b)			59.1-581.4			2.1 30.3	APP Part 11		7(c) 7(d) 7(e) 8(5) 8(6)		Principle 7
				Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5		CC1.3-POF4 CC1.5 CC4.1 CC4.2-POF1 CC4.2-POF2 CC4.2-POF3			10.2 10.2(a) 10.2(b) 10.2(c) 10.2(d) 10.2(e)	6.12												712(b)(3)											
				Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5		CC2.2-POF11 CC5.1-POF2			4.3	6.12				GV.SC-05								712(b)(2) 712(b)(d).E						2.2					
				Intersects With	Ability To Demonstrate Conformity	CPL-01.3	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5	updated in 2026.1 release					6.12						8.7.b 8.5.a			712(c) 712(b)(d).D					5.2 30.4 30.4 31	30.4.a					
				Intersects With	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5	updated in 2026.1 release					6.12									712(e) 712(f)(1) 712(f)(2) 712(f)(3) 712(f) 712(f)(4) 712(f)(5) 712(f)(6) 712(f) 712(f)(6)(i) 712(h)						59.1-579.B.4							
				Intersects With	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5		CI.2						AU-11	AU-11																			
				Intersects With	Computer-Matching Agreements (CMA)	PRI-02.3	Mechanisms exist to publish Computer Matching Agreements (CMA) on the organization's public website(s).	5								PM-24 PT-8	PM-24 PT-8																			
				Intersects With	System of Records Notice (SORN)	PRI-02.4	Mechanisms exist to draft, publish and keep System of Records Notices (SORN) updated in accordance with regulatory guidance.	5								PT-6	PT-6																			
				Intersects With	System of Records Notice (SORN) Review Process	PRI-02.5	Mechanisms exist to review all routine uses of data published in the System of Records Notices (SORN) to ensure continued accuracy and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.	5								PT-6(1)	PT-6(1)																			
				Intersects With	Privacy Act Exemptions	PRI-02.6	Mechanisms exist to review all Privacy Act exemptions claimed for the System of Records Notices (SORN) to ensure they remain appropriate and accurate.	5								PT-6(2)	PT-6(2)																			
11.7	Critical Business Functions	Ensure Technology Assets, Applications and/or Services (TAAS) that support organizational priorities are assessed so that critical assets are identified and key functional requirements communicated.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5		CC7.5					ID.BE-P3	CP-2(8)			GV.OC-04 GV.SC-05 ID.AM-05 ID.RA-04 RC.RP-02 RC.RP-04				164.308(a)(7)(ii)(E)																	
				Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5		P11.1					ID.BE-P3	PM-30(1) RA-9 SA-15(3)								712(b)(3)(4)												
				Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		CC3.2-POF8 CC3.2-POF9 CC9.1					ID.BE-P3	PM-30(1) RA-9 SA-9(3)			GV.OC-04 GV.SC-05 GV.SC-06 GV.SC-07 GV.SC-07 GV.SC-08 ID.AM-05 ID.RA-10				164.308(a)(7)(ii)(E)			712(b)(3)(5)												
11.8	Status Reporting To Governing Body	Provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data privacy program.	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5		CC2.2-POF2 CC2.2-POF3 CC2.3-POF5 CC3.1-POF10 CC3.1-POF11 CC4.2 CC4.2-POF1 CC4.2-POF2			5.1 5.2(b) 9.3.1					GV.OV GV.OV-03 GV.SC-07 GV.SC GV.SC-09 ID																			30(2)(c)(ii)			