

| 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          | Legacy SCF # |
|-------|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------|-------------------------------------------------------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------|--------------|
| 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-02   | Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 5                        |                | GOV-01       |
| 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-02   | 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                        |                | PRI-01       |
| 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-09   | 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 appropriate.                                                                                                                                                                                                                                                                                                                                                                                                                     | 5                        |                | PRI-01.11    |
| 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-20   | Mechanisms exist to:<br>(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;<br>(2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories;<br>(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<br>(4) Inform data subjects when changes are made to the privacy notice and the nature of such changes. | 5                        |                | PRI-01.3     |
| 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-02   | 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                        |                | PRI-01       |
| 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 Accountability Structure                             | PRI-03   | Mechanisms exist to establish a data privacy accountability structure that:<br>(1) Identifies data privacy roles required by applicable statutory, regulatory and/or contractual obligations;<br>(2) Assigns each role to one or more individuals with the requisite qualifications, authority, independence and resources; and<br>(3) Is reviewed and updated as data privacy obligations, operating jurisdictions and/or business practices change.                                                                                                                                                                                                    | 8                        | Updated 2026.3 |              |
| 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   | Chief Privacy Officer (CPO)                                       | PRI-03.1 | Mechanisms exist to identify and appoint a Chief Privacy Officer (CPO), or equivalent 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                        |                | PRI-01.1     |
| 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-03.2 | Mechanisms exist to identify and appoint a Data Protection Officer (DPO), or equivalent role:<br>(1) Based on professional qualifications; and<br>(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                        |                | PRI-01.4     |
| 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-04   | Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 5                        |                | DCH-02       |
| 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-06   | Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 5                        |                | PRI-05.7     |
| 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-45   | 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                        |                | PRI-15       |
| 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-04   | Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 5                        |                | PRM-01       |
| 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-07   | 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                        |                | PRI-05.5     |
| 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-07.1 | Automated mechanisms exist to determine if Personal Data (PD) is maintained in electronic form.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 5                        |                | PRI-05.6     |
| 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-02   | Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 5                        |                | SAT-01       |
| 1.6   | Data Privacy Training                   | Provide recurring data privacy awareness and training for all employees and contractors.                                                                                                                                                                                                                    | Functional     | Intersects With   | Security, Compliance & Resilience Awareness Training              | SAT-04   | 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                        |                | SAT-02       |
| 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-04.1 | Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 5                        |                | SAT-02.1     |
| 1.6   | Data Privacy Training                   | Provide recurring data privacy awareness and training for all employees and contractors.                                                                                                                                                                                                                    | Functional     | Intersects With   | Role-Based Security, Compliance & Resilience Training             | SAT-05   | Mechanisms exist to provide role-based security, compliance and resilience-related training:<br>(1) Before authorizing access to the system or performing assigned duties;<br>(2) When required by system changes; and<br>(3) Annually thereafter.                                                                                                                                                                                                                                                                                                                                                                                                       | 5                        |                | SAT-03       |
| 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-05.1 | Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive and/or regulated data is formally trained in data handling requirements.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 5                        |                | SAT-03.3     |
| 1.6   | Data Privacy Training                   | Provide recurring data privacy awareness and training for all employees and contractors.                                                                                                                                                                                                                    | Functional     | Intersects With   | Cyber Threat Environment Situational Awareness                    | SAT-06   | 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                        |                | SAT-03.6     |
| 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-06.2 | Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 5                        |                | SAT-03.2     |
| 1.6   | Data Privacy Training                   | Provide recurring data privacy awareness and training for all employees and contractors.                                                                                                                                                                                                                    | Functional     | Intersects With   | Practical Security Training Exercises                             | SAT-09   | Mechanisms exist to include practical exercises in security, compliance and resilience training that reinforce training objectives.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 5                        |                | SAT-03.1     |
| 1.6   | Data Privacy Training                   | Provide recurring data privacy awareness and training for all employees and contractors.                                                                                                                                                                                                                    | Functional     | Intersects With   | Security, Compliance & Resilience Training Records                | SAT-10   | Mechanisms exist to document, retain and monitor individual training activities, including:<br>(1) Initial security, compliance and resilience awareness training;<br>(2) Recurring awareness training; and<br>(3) Technology Assets, Applications and/or Services (TAAS)-specific training.                                                                                                                                                                                                                                                                                                                                                             | 5                        |                | SAT-04       |
| 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-06   | Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 5                        |                | PRI-05.7     |
| 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-37   | Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 5                        |                | PRI-17       |
| 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-21.2 | Mechanisms exist to include a conspicuous link to the organization's data privacy notice on all consumer-facing websites and mobile applications.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 5                        |                | PRI-17.1     |
| 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-19.1 | 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.                                                                                                                                                                                                                                                                                                                                                                                                    | 5                        |                | PRI-17.2     |

| 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          | Legacy SCF # |
|-------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------|-----------------------------------------------------------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------|--------------|
| 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   | Data Subject Consent                                                  | PRI-24   | Mechanisms exist to enable data subjects to authorize the collection, receipt, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where the data subject is provided, prior to collection, with:<br>(1) Plain language explaining the potential data privacy risks of the authorization;<br>(2) A means to decline the authorization; and<br>(3) Necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations. | 5                        |                | PRI-03       |
| 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   | Data Subject Consent                                                  | PRI-24   | Mechanisms exist to enable data subjects to authorize the collection, receipt, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where the data subject is provided, prior to collection, with:<br>(1) Plain language explaining the potential data privacy risks of the authorization;<br>(2) A means to decline the authorization; and<br>(3) Necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations. | 5                        |                | PRI-03       |
| 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   | Data Subject Consent                                                  | PRI-24   | Mechanisms exist to enable data subjects to authorize the collection, receipt, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where the data subject is provided, prior to collection, with:<br>(1) Plain language explaining the potential data privacy risks of the authorization;<br>(2) A means to decline the authorization; and<br>(3) Necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations. | 5                        |                | PRI-03       |
| 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   | Data Subject Opt-In Consent                                           | PRI-27   | Mechanisms exist to obtain consent from data subjects to opt-in for the following Personal Data (PD) actions:<br>(1) Collecting;<br>(2) Receiving;<br>(3) Processing;<br>(4) Storing;<br>(5) Transmitting;<br>(6) Sharing; and/or<br>(7) Updating.                                                                                                                                                                                                                                                                      | 8                        | Updated 2026.3 | PRI-03.12    |
| 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-24.3 | Mechanisms exist to allow data subjects to revoke consent to collect, receive, process, store, transmit, share and/or update their Personal Data (PD).                                                                                                                                                                                                                                                                                                                                                                  | 5                        |                | PRI-03.4     |
| 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-24.4 | 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:<br>(1) The original circumstances under which an individual gave consent have changed; or<br>(2) A significant amount of time has passed since an individual gave consent.                                                                                                                    | 5                        |                | PRI-03.2     |
| 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-02   | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.                                                                                                                                                                                                                                                                                                                                                                                        | 5                        |                | CPL-01       |
| 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-13   | Mechanisms exist to prevent discrimination against a data subject for exercising their legal rights pertaining to modifying or revoking consent, including prohibiting:<br>(1) Refusing products and/or services;<br>(2) Charging different rates for goods and/or services; and<br>(3) Providing different levels of quality.                                                                                                                                                                                          | 5                        |                | PRI-03.5     |
| 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-24.2 | 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                        |                | PRI-03.1     |
| 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-24.5 | Mechanisms exist to prevent the sale, processing and/or sharing of Personal Data (PD) when:<br>(1) Instructed by the data subject; or<br>(2) The data subject is a minor, where selling and/or sharing PD is legally prohibited.                                                                                                                                                                                                                                                                                        | 5                        |                | PRI-03.3     |
| 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-28   | Mechanisms exist to allow data subjects to authorize another person or entity (e.g., authorized agent and proxy), acting on the data subject's behalf, to make Personal Data (PD) processing decisions.                                                                                                                                                                                                                                                                                                                 | 5                        |                | PRI-03.6     |
| 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-26.3 | Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).                                                                                                                                                                                                                                                                                                                                                                             | 5                        |                | PRI-03.8     |
| 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, Processing & Sharing To Identified Purpose       | PRI-31.1 | Mechanisms exist to minimize the collection, processing and/or sharing of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.                                                                                                                                                                                                      | 5                        |                | PRI-04       |
| 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-12   | 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.                                                                                                                                                                                                                                                             | 5                        |                | PRI-04.1     |
| 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-28   | Mechanisms exist to minimize the use of sensitive and/or regulated data for research, testing, or training, in accordance with authorized, legitimate business practices.                                                                                                                                                                                                                                                                                                                                               | 5                        |                | DCH-18.2     |
| 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 Exposure                          | DCH-27.1 | Mechanisms exist to minimize sensitive and/or 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                        |                | DCH-18.1     |
| 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-29   | Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:<br>(1) The purpose(s) originally collected, consistent with the data privacy notice(s);<br>(2) What is authorized by the data subject, or authorized agent; and<br>(3) What is consistent with applicable laws, regulations and contractual obligations.                                                                                                                          | 5                        |                | PRI-05.4     |
| 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-29.3 | Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that:<br>(1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and<br>(2) Authorizes the use of PD when such information is required for internal testing, training and research.                                                                                                                                                                   | 5                        |                | PRI-05.1     |
| 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 Requests To Data Subject                   | PRI-18   | Mechanisms exist to notify data subjects of applicable legal requests to disclose Personal Data (PD).                                                                                                                                                                                                                                                                                                                                                                                                                   | 5                        |                | PRI-14.2     |

| 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 | Legacy SCF # |
|-------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------|-----------------------------------------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|-------|--------------|
| 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-20.1 | Mechanisms exist to provide additional formal notice to individuals from whom the information is being collected that includes:<br>(1) Notice of the authority of organizations to collect Personal Data (PD);<br>(2) Whether providing PD is mandatory or optional;<br>(3) The principal purpose or purposes for which the PD is to be used;<br>(4) The intended disclosures or routine uses of the information; and<br>(5) The consequences of not providing all or some portion of the information requested.                                                                                                                                                                                                                                                                                                                                                                                               | 5                        |       | PRI-01.2     |
| 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-21   | Mechanisms exist to:<br>(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;<br>(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;<br>(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;<br>(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;<br>(5) Periodically, review and update the content of the privacy notice, as necessary; and<br>(6) Retain prior versions of the privacy notice, in accordance with data retention requirements. | 5                        |       | PRI-02       |
| 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 Requests To Data Subject | PRI-18   | Mechanisms exist to notify data subjects of applicable legal requests to disclose Personal Data (PD).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 5                        |       | PRI-14.2     |
| 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-22   | 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                        |       | PRI-02.1     |
| 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-02   | Mechanisms exist to facilitate the implementation of data protection controls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 5                        |       | DCH-01       |
| 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-30   | Mechanisms exist to:<br>(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;<br>(2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and<br>(3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 5                        |       | PRI-05       |
| 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 Decision-Making Technology (ADMT)         | PRI-36   | 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                        |       | PRI-02.2     |
| 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-05.1 | 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                        |       | PRI-09       |
| 5.2   | Data Flow Mapping                           | Maintain a record of processing activities that documents the flow of personal data that includes:<br>- Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data;<br>- Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data;<br>- The purposes of the storage, transmission and processing;<br>- A description of the categories of data subjects and personal data;<br>- Where possible, the time limits for erasure of the different categories of data; and<br>- Where possible, a description of the cybersecurity & data privacy measures of the data controller. | Functional     | Intersects With   | Asset Inventories                                   | AST-04   | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:<br>(1) Accurately reflects the current TAASD in use;<br>(2) Identifies authorized software products, including business justification details;<br>(3) Is at the level of granularity deemed necessary for tracking and reporting;<br>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and<br>(5) Is available for review and audit by designated organizational personnel.                                                                                                                                                                                                                                                                                                                                                          | 5                        |       | AST-02       |
| 5.2   | Data Flow Mapping                           | Maintain a record of processing activities that documents the flow of personal data that includes:<br>- Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data;<br>- Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data;<br>- The purposes of the storage, transmission and processing;<br>- A description of the categories of data subjects and personal data;<br>- Where possible, the time limits for erasure of the different categories of data; and<br>- Where possible, a description of the cybersecurity & data privacy measures of the data controller. | Functional     | Intersects With   | Network Diagrams & Data Flow Diagrams (DFDs)        | AST-17   | Mechanisms exist to maintain network architecture diagrams that:<br>(1) Contain sufficient detail to assess the security of the network's architecture;<br>(2) Reflect the current architecture of the network environment; and<br>(3) Document all sensitive and/or regulated data flows.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 5                        |       | AST-04       |
| 5.2   | Data Flow Mapping                           | Maintain a record of processing activities that documents the flow of personal data that includes:<br>- Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data;<br>- Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data;<br>- The purposes of the storage, transmission and processing;<br>- A description of the categories of data subjects and personal data;<br>- Where possible, the time limits for erasure of the different categories of data; and<br>- Where possible, a description of the cybersecurity & data privacy measures of the data controller. | Functional     | Intersects With   | Data Action Mapping                                 | AST-17.2 | Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive and/or regulated data is stored, transmitted or processed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 5                        |       | AST-02.8     |
| 5.2   | Data Flow Mapping                           | Maintain a record of processing activities that documents the flow of personal data that includes:<br>- Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data;<br>- Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data;<br>- The purposes of the storage, transmission and processing;<br>- A description of the categories of data subjects and personal data;<br>- Where possible, the time limits for erasure of the different categories of data; and<br>- Where possible, a description of the cybersecurity & data privacy measures of the data controller. | Functional     | Intersects With   | Sensitive / Regulated Media Records                 | DCH-10   | Mechanisms exist to ensure media records for sensitive and/or regulated data contain sufficient information to determine the potential impact in the event of a data loss incident.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 5                        |       | DCH-01.3     |
| 5.2   | Data Flow Mapping                           | Maintain a record of processing activities that documents the flow of personal data that includes:<br>- Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data;<br>- Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data;<br>- The purposes of the storage, transmission and processing;<br>- A description of the categories of data subjects and personal data;<br>- Where possible, the time limits for erasure of the different categories of data; and<br>- Where possible, a description of the cybersecurity & data privacy measures of the data controller. | Functional     | Intersects With   | Data Modeling Guidelines                            | DCH-34   | Mechanisms exist to issue data modeling guidelines to support tagging of sensitive and/or regulated data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 5                        |       | PRI-11       |

| 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          | Legacy SCF # |
|-------|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------|------------------------------------------------------------------------------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------|--------------|
| 5.2   | Data Flow Mapping                   | Maintain a record of processing activities that documents the flow of personal data that includes:<br>- Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data;<br>- Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data;<br>- The purposes of the storage, transmission and processing;<br>- A description of the categories of data subjects and personal data;<br>- Where possible, the time limits for erasure of the different categories of data; and<br>- Where possible, a description of the cybersecurity & data privacy measures of the data controller. | Functional     | Intersects With   | Sensitive / Regulated Data Actions                                                 | IAC-49.1 | Automated mechanisms exist to generate event logs whenever sensitive and/or regulated data is collected, created, updated, deleted and/or archived.                                                                                                                                                                                                                                                                 | 5                        |                | CFG-08.1     |
| 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   | Technology Assets, Applications, Services and/or Data (TAASD) Ownership Assignment | AST-07.1 | Mechanisms exist to ensure Technology Assets, Applications, Services and/or Data (TAASD) 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                        |                | AST-03       |
| 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-07.2 | Mechanisms exist to formally document the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.                                                                                                                                                                                                                             | 5                        |                | AST-03.1     |
| 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-27   | Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.                                                                                                                                                                                                                                                                                          | 5                        |                | DCH-18       |
| 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 Exposure                                       | DCH-27.1 | Mechanisms exist to minimize sensitive and/or 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                        |                | DCH-18.1     |
| 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   | Digital & Non-Digital Media Disposal                                               | DCH-17   | Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.                                                                                                                                                                                                                                                   | 5                        |                | DCH-21       |
| 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 Sensitive / Regulated Data                                         | DCH-18.1 | Mechanisms exist to facilitate the sanitization of sensitive and/or regulated data.                                                                                                                                                                                                                                                                                                                                 | 5                        |                | DCH-09.3     |
| 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   | Logical Data Location                                                              | DCH-29   | Mechanisms exist to identify and document the logical location of data and the specific Technology Assets, Applications and/or Services (TAAS) on which the data resides.                                                                                                                                                                                                                                           | 5                        |                | DCH-24       |
| 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   | Geolocation Requirements for Processing, Storage and Service Locations             | DCH-30.1 | Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.                                                                                                                                                                                        | 8                        | Updated 2026.3 | CLD-09       |
| 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   | External Transfer of Sensitive / Regulated Data                                    | DCH-32   | Mechanisms exist to restrict and govern the transfer of sensitive and/or regulated data:<br>(1) Cross-border; and/or<br>(2) Interorganizational.                                                                                                                                                                                                                                                                    | 5                        |                | DCH-25       |
| 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-25   | Mechanisms exist to distribute processing and storage across multiple physical locations.                                                                                                                                                                                                                                                                                                                           | 5                        |                | SEA-15       |
| 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-12.2 | Mechanisms exist to restrict the location of information processing/storage based on business requirements.                                                                                                                                                                                                                                                                                                         | 5                        |                | TPM-04.4     |
| 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-41   | 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                        |                | PRI-06.6     |
| 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-41.1 | Mechanisms exist to export a data subject's available Personal Data (PD) in a readily usable format, upon an authenticated request.                                                                                                                                                                                                                                                                                 | 5                        |                | PRI-06.7     |
| 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-05   | 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                        |                | PRI-14       |
| 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-17.1 | Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:<br>(1) The organization; and/or<br>(2) Relevant third-parties that their PD was shared with.                                                                                                                                                                                                 | 5                        |                | PRI-14.1     |
| 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   | Sensitive / Regulated Data Governance                                              | DCH-03   | Mechanisms exist to facilitate data governance so that sensitive and/or regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.                                                                                                                                                                                                       | 5                        |                | GOV-10       |
| 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-35   | Mechanisms exist to ensure the accuracy and relevance of Personal Data (PD) throughout the information lifecycle by:<br>(1) Keeping PD up-to-date; and<br>(2) Remediating identified inaccuracies, as necessary.                                                                                                                                                                                                    | 5                        |                | PRI-05.2     |
| 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-36   | Mechanisms exist to de-identify sensitive and/or regulated data through<br>(1) Anonymization;<br>(2) De-identification;<br>(3) Pseudonymization; and/or<br>(4) Redaction.                                                                                                                                                                                                                                           | 5                        |                | DCH-23       |
| 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                                                            | DCH-33.2 | Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive and/or regulated data across the information lifecycle.                                                                                                                                                                                                                         | 5                        |                | PRI-10       |
| 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                                                            | DCH-33.3 | Automated mechanisms exist to support the evaluation of data quality across the information lifecycle.                                                                                                                                                                                                                                                                                                              | 5                        |                | PRI-10.1     |
| 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                        |                | PRM-07       |
| 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-08   | Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.                                                                                                | 5                        |                | PRM-04       |
| 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 Requirements Definition                          | PRM-09   | Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by:<br>(1) Defining technical security, compliance and resilience requirements; and<br>(2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).                                                                                                               | 5                        |                | PRM-05       |
| 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-10   | Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:<br>(1) The resulting risk to organizational operations, assets, individuals and other organizations; and<br>(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                        |                | PRM-06       |
| 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-11   | Mechanisms exist to manage the organizational knowledge of the security, compliance and resilience staff.                                                                                                                                                                                                                                                                                                           | 5                        |                | PRM-08       |

| 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          | Legacy SCF # |
|-------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------|--------------------------------------------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------|--------------|
| 5.12  | Secure Data Processing              | Implement secure data processing practices so that the confidentiality, integrity and pertinent attributes of sensitive/regulatory data is maintained throughout the data lifecycle.                       | Functional     | Intersects With   | Secure Engineering Principles                                      | SEA-05   | 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                        |                | SEA-01       |
| 5.12  | Secure Data Processing              | Implement secure data processing practices so that the confidentiality, integrity and pertinent attributes of sensitive/regulatory data is maintained throughout the data lifecycle.                       | Functional     | Intersects With   | Secure Software Development Practices (SSDP)                       | TDA-05   | Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 5                        |                | TDA-06       |
| 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-09   | Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(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<br>(3) Provides a historical record of applied security controls, including changes.                                                                                                                                                                                                                                                                                      | 5                        |                | IAO-03       |
| 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-05.1 | 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                        |                | PRI-09       |
| 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-24.4 | 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:<br>(1) The original circumstances under which an individual gave consent have changed; or<br>(2) A significant amount of time has passed since an individual gave consent.                                                                                                                                                                                                                                                                                                                                                                                                                                          | 5                        |                | PRI-03.2     |
| 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   | Automated Decision-Making Technology (ADMT)                        | PRI-36   | 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).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 8                        | Updated 2026.3 | PRI-02.2     |
| 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)                           | PRI-08.1 | 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                        |                | DCH-22.1     |
| 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)                           | PRI-08.2 | Mechanisms exist to identify and correct flaws related to the collection, usage, processing or dissemination of Personal Data (PD).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 5                        |                | VPM-04.2     |
| 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-12   | 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                        |                | THR-06       |
| 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 (VPM)                     | VPM-02   | Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 5                        |                | VPM-01       |
| 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-03   | Mechanisms exist to define and manage the scope for its attack surface management activities.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 5                        |                | VPM-01.1     |
| 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-05   | Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 5                        |                | VPM-03       |
| 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-06   | Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 5                        |                | VPM-02       |
| 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-06.2 | Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 5                        |                | VPM-04       |
| 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-08   | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 5                        |                | VPM-05       |
| 5.16  | Analytical Biases                   | Understand and evaluate data analytic inputs and outputs for potential bias.                                                                                                                               | Functional     | Intersects With   | Data Analytics Bias                                                | DCH-35   | Mechanisms exist to evaluate its analytical processes for potential bias.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 5                        |                | PRI-10.2     |
| 6     | Data Subject Rights                 | Provide data subjects with appropriate access to their personal data.                                                                                                                                      | Functional     | Intersects With   | Disclosure Request Rejections                                      | PRI-18.1 | Mechanisms exist to reject disclosure requests that are:<br>(1) Unjustified;<br>(2) Unauthenticated or untrustworthy; and/or<br>(3) Unlawful.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 5                        |                | PRI-07.4     |
| 6     | Data Subject Rights                 | Provide data subjects with appropriate access to their personal data.                                                                                                                                      | Functional     | Intersects With   | Active Participation For Consent By Data Subjects                  | PRI-24.1 | 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 and accept all cookies).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 5                        |                | PRI-03.7     |
| 6     | Data Subject Rights                 | Provide data subjects with appropriate access to their personal data.                                                                                                                                      | Functional     | Intersects With   | Data Subject Empowerment                                           | PRI-39.1 | Mechanisms exist to provide authenticated data subjects the ability to:<br>(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;<br>(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;<br>(3) Obtain the source(s) of their PD;<br>(4) Obtain the categories of their PD being collected, received, processed, stored and shared;<br>(5) Request correction to their PD due to inaccuracies;<br>(6) Request erasure of their PD; and<br>(7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD. | 5                        |                | PRI-06       |
| 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)                           | PRI-08.1 | 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                        |                | DCH-22.1     |
| 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   | Disclosure Request Rejections                                      | PRI-18.1 | Mechanisms exist to reject disclosure requests that are:<br>(1) Unjustified;<br>(2) Unauthenticated or untrustworthy; and/or<br>(3) Unlawful.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 5                        |                | PRI-07.4     |
| 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   | Data Subject Authentication                                        | PRI-38   | 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                        |                | PRI-06.8     |
| 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 Rights Management                                     | PRI-39   | Mechanisms exist to facilitate the receipt, validation, fulfillment and documentation of data subject rights requests in accordance with applicable statutory, regulatory and/or contractual obligations.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 5                        |                | PRI-06.4     |
| 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) Process                                | PRI-08   | Mechanisms exist to identify and record:<br>(1) The process(es) used to update Personal Data (PD); and<br>(2) The frequency that such updates occur.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 5                        |                | PRI-12       |
| 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)                           | PRI-08.1 | 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                        |                | DCH-22.1     |
| 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-39.3 | Mechanisms exist to maintain a process for:<br>(1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and<br>(2) Disseminating corrections or amendments of PD to other authorized users of the PD.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 5                        |                | PRI-06.1     |

| 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 | Legacy SCF # |
|-------|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------|----------------------------------------------------------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|-------|--------------|
| 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-39.4 | Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected, amended or deleted.                                                                                                                                                                                                                                                                                             | 5                        |       | PRI-06.2     |
| 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-42   | Mechanisms exist to inform applicable third-parties of any modification, deletion or other change that affects shared Personal Data (PD).                                                                                                                                                                                                                                                                         | 5                        |       | PRI-07.3     |
| 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-39.5 | Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.                                                                                                                                                                                                                                                                                                                           | 5                        |       | PRI-06.3     |
| 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-40   | 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                        |       | PRI-06.5     |
| 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 Security, Compliance & Resilience Controls | GOV-03   | Mechanisms exist to centrally-manage security, compliance and resilience: (1) Controls; and (2) Related processes.                                                                                                                                                                                                                                                                                                | 5                        |       | SEA-01.1     |
| 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-11   | Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.                                                                                                                                                                                                      | 5                        |       | GOV-15       |
| 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-11.1 | Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.                                                                                                                                                                                                      | 5                        |       | GOV-15.1     |
| 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-11.2 | Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.                                                                                                                                                                                                   | 5                        |       | GOV-15.2     |
| 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-11.3 | Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control are: (1) Designed to meet control objectives; (2) Implemented correctly; and (3) Operating as intended.                                                                                            | 5                        |       | GOV-15.3     |
| 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-11.4 | 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                        |       | GOV-15.4     |
| 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-11.5 | 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                        |       | GOV-15.5     |
| 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-02   | Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.                                                                                                                                                                                                                                                                                                         | 5                        |       | IAC-01       |
| 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-02   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.                                                                                                                                                                                                                                                                                                                         | 5                        |       | MON-01       |
| 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 Event Logs & Security-Relevant Telemetry   | MON-05   | Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.                                                                                                                                                                                                                             | 5                        |       | MON-02       |
| 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-10   | 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                        |       | PRI-01.6     |
| 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-02   | Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.                                                                                                                                                                                                                                       | 5                        |       | TDA-01       |
| 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, Compliance & Resilience Testing Throughout Development     | TDA-17   | 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                        |       | TDA-09       |
| 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-03   | Mechanisms exist to govern the technical configuration change control processes.                                                                                                                                                                                                                                                                                                                                  | 5                        |       | CHG-02       |
| 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-06   | Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.                                                                                                                                                                                                                                                                                           | 5                        |       | CHG-03       |
| 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-02   | Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.                                                                                                                                                                                                                                                          | 5                        |       | CLD-01       |
| 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-05   | Mechanisms exist to ensure that the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud deployments.                                                                                                                                                                                                                                     | 5                        |       | CLD-02       |
| 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 Security, Compliance & Resilience Capabilities      | GOV-11   | Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.                                                                                                                                                                                                      | 5                        |       | GOV-15       |
| 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-11.1 | Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.                                                                                                                                                                                                      | 5                        |       | GOV-15.1     |
| 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-11.2 | Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.                                                                                                                                                                                                   | 5                        |       | GOV-15.2     |

| 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 | Legacy SCF # |
|-------|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------|-----------------------------------------------------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|-------|--------------|
| 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-11.3 | Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control are:<br>(1) Designed to meet control objectives;<br>(2) Implemented correctly; and<br>(3) Operating as intended.                                                                                                                                    | 5                        |       | GOV-15.3     |
| 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-11.4 | 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                        |       | GOV-15.4     |
| 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-11.5 | 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                        |       | GOV-15.5     |
| 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-03   | Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).                                                                                                                                                                                                                                                                                         | 5                        |       | IAC-01.2     |
| 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-06   | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.                                                                                                                                                                                                                                           | 5                        |       | IAC-08       |
| 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-09   | Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.                                                                                                                                                                                                                                                                                                                                      | 5                        |       | IAC-28.1     |
| 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-10   | Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).                                                                                                                                                                                                                                                                                                                            | 5                        |       | IAC-16       |
| 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-30   | Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.                                                                                                                                                                                                                                                              | 5                        |       | IAC-21       |
| 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-37   | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:<br>(1) Remote network access;<br>(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or<br>(3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.                                                                                                                                                       | 5                        |       | IAC-06       |
| 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-10   | 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                        |       | PRI-01.6     |
| 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-04   | Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.                                                                                                                                                                                   | 5                        |       | SEA-02       |
| 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-05   | 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                        |       | SEA-01       |
| 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-03   | 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.                                                                                                                                                                     | 5                        |       | TDA-02.3     |
| 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-05   | Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).                                                                                                                                                                                                                                                                                                                                                                    | 5                        |       | TDA-06       |
| 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-05.4 | Mechanisms exist to have an independent review of the software design to validate:<br>(1) Applicable security, compliance and resilience requirements are met; and<br>(2) Identified risks are remediated.                                                                                                                                                                                                                                                         | 5                        |       | TDA-06.5     |
| 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-06   | 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:<br>(1) Improve functionality;<br>(2) Enhance security and resiliency capabilities;<br>(3) Correct security deficiencies; and<br>(4) Conform with applicable statutory, regulatory and/or contractual obligations. | 5                        |       | TDA-01.1     |
| 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-06.3 | Mechanisms exist to deliver security updates to Technology Assets, Applications and/or Services (TAAS), where applicable, through:<br>(1) Automatic updates; and<br>(2) Notification of available updates to affected users.                                                                                                                                                                                                                                       | 5                        |       | TDA-02.9     |
| 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-07   | Mechanisms exist to disclose information about vulnerabilities to relevant stakeholders, including:<br>(1) A description of the vulnerability(ies);<br>(2) Affected product(s) and/or service(s);<br>(3) Potential impact of the vulnerability(ies);<br>(4) Severity of the vulnerability(ies); and<br>(5) Guidance to remediate the vulnerability(ies).                                                                                                           | 5                        |       | TDA-02.11    |
| 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-08   | 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.                                                                                                                                                                                                | 5                        |       | TDA-22       |
| 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-11.2 | Mechanisms exist to mitigate the risk associated with the use of insecure ports, protocols and services necessary to operate technology solutions.                                                                                                                                                                                                                                                                                                                 | 5                        |       | TDA-02.6     |
| 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-13   | Mechanisms exist to minimize the attack surface of Technology Assets, Applications and/or Services (TAAS) by reasonably mitigating known exploitable vulnerabilities.                                                                                                                                                                                                                                                                                              | 5                        |       | TDA-02.8     |
| 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-13.1 | Mechanisms exist to ensure vendors / manufacturers:<br>(1) Deliver the Technology Asset, Application and/or Service (TAAS) with a pre-established, secure configuration implemented; and<br>(2) Use the pre-established, secure configuration as the default for any subsequent TAAS reinstallation or upgrade.                                                                                                                                                    | 5                        |       | TDA-02.4     |
| 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-14   | 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.                                                                                                                                                                                                                                                                             | 5                        |       | TDA-02.10    |
| 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, Compliance & Resilience Representatives For Product Changes | TDA-14.1 | Mechanisms exist to include appropriate security, compliance and resilience representatives in the product feature and/or functionality change control review process.                                                                                                                                                                                                                                                                                             | 5                        |       | TDA-02.7     |

| 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          | Legacy SCF # |
|-------|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------|---------------------------------------------------------------------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------|--------------|
| 7.2   | Cryptographic Protections                       | Ensure personal data is encrypted both at rest and in transit.                                                                                                                                                                                                                                                                                                                     | Functional     | Intersects With   | Use of Cryptographic Controls                                                   | CRY-02   | Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.                                                                                                                                                                                                                                                               | 5                        |                | CRY-01       |
| 7.2   | Cryptographic Protections                       | Ensure personal data is encrypted both at rest and in transit.                                                                                                                                                                                                                                                                                                                     | Functional     | Intersects With   | Encrypting Data In Transit                                                      | CRY-05   | Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.                                                                                                                                                                                                                                                                                                                                  | 5                        |                | CRY-03       |
| 7.2   | Cryptographic Protections                       | Ensure personal data is encrypted both at rest and in transit.                                                                                                                                                                                                                                                                                                                     | Functional     | Intersects With   | Encrypting Data At Rest                                                         | CRY-07   | Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.                                                                                                                                                                                                                                                                                                                                     | 5                        |                | CRY-05       |
| 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-02   | Mechanisms exist to facilitate the operation of physical and environmental protection controls.                                                                                                                                                                                                                                                                                                                            | 5                        |                | PES-01       |
| 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-06   | Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).                                                                                                                                                                                            | 5                        |                | PES-02       |
| 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-07   | Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.                                                                                                                                                                                                                                                                                       | 5                        |                | PES-02.1     |
| 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-08   | Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).                                                                                                                                                         | 5                        |                | PES-03       |
| 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-10   | 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.                                                                                                                                                                                    | 5                        |                | PES-04       |
| 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-13   | Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.                                                                                                                                                                                                                                                                                                                | 5                        |                | PES-05       |
| 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-14   | Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).                                                                                                                                                                                                                                          | 5                        |                | PES-06       |
| 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 Sensor Data Use Restrictions                                           | CFG-18.1 | Mechanisms exist to ensure data collected by embedded sensors is restricted to authorized purposes.                                                                                                                                                                                                                                                                                                                        | 5                        |                | END-13.1     |
| 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 Embedded Sensor Data Collection                                       | CFG-18.2 | Mechanisms exist to notify individuals of embedded sensor data collection.                                                                                                                                                                                                                                                                                                                                                 | 5                        |                | END-13.2     |
| 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 Sensor Data Collection Minimization                                    | CFG-18.3 | Mechanisms exist to utilize embedded sensors that are configured to minimize the collection of information about individuals.                                                                                                                                                                                                                                                                                              | 5                        |                | END-13.3     |
| 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-02   | Mechanisms exist to facilitate the implementation of embedded technology controls.                                                                                                                                                                                                                                                                                                                                         | 5                        |                | EMB-01       |
| 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)              | AST-39   | Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by:<br>(1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and<br>(2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.                               | 5                        |                | TDA-17       |
| 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   | Human Resources Security Management                                             | HRS-02   | Mechanisms exist to facilitate the implementation of personnel security controls.                                                                                                                                                                                                                                                                                                                                          | 5                        | Updated 2026.3 | HRS-01       |
| 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-06.1 | Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.                                                                                                                                                                                                                                                                    | 5                        |                | HRS-05.1     |
| 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-06.2 | 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.                                                                                                                                                                                                               | 5                        |                | HRS-05.2     |
| 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-10   | Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.                                                                                                                                                                                                                                                                                                     | 5                        |                | HRS-07       |
| 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-02   | Mechanisms exist to facilitate the implementation of personnel security controls.                                                                                                                                                                                                                                                                                                                                          | 5                        |                | HRS-01       |
| 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   | Security, Compliance & Resilience-Minded                                        | SAT-02   | Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.                                                                                                                                                                                                                                                                                                                | 5                        | Updated 2026.3 | SAT-01       |
| 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   | Competency Requirements for Security, Compliance & Resilience-Related Positions | HRS-03.2 | Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.                                                                                                                                                                                                                                                           | 8                        | Updated 2026.3 | HRS-03.2     |
| 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-05   | Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.                                                                                                                                                                                                                                                                                                                   | 5                        |                | HRS-04       |
| 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-02   | Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.                                                                                                                                                                                                                                                                                            | 5                        |                | IAO-01       |
| 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-14   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.                                                                                                                                                                                                                                                                | 5                        |                | IAO-07       |
| 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-22   | Mechanisms exist to monitor risk as an integral part of the continuous monitoring strategy, including:<br>(1) The effectiveness of security, compliance and resilience controls;<br>(2) Changes to the organization's risk profile; and<br>(3) Changes to Technology Assets, Applications and/or Services (TAAS) that affect risk.                                                                                         | 5                        |                | RSK-11       |
| 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, Compliance & Resilience Testing Throughout Development                | TDA-17   | Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:<br>(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;<br>(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and<br>(3) Document the results. | 5                        |                | TDA-09       |
| 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-02   | Mechanisms exist to facilitate the implementation of configuration management controls.                                                                                                                                                                                                                                                                                                                                    | 5                        |                | CFG-01       |
| 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-04   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.                                                                                                                                                                                                               | 5                        |                | CFG-02       |

| 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          | Legacy SCF # |
|-------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------|--------------------------------------------------------------------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------|--------------|
| 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   | Security, Compliance & Resilience Testing Throughout Development               | TDA-17   | Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:<br>(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;<br>(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and<br>(3) Document the results. | 5                        |                | TDA-09       |
| 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   | System Generated Event Logs & Security-Relevant Telemetry                      | MON-04   | Mechanisms exist to generate, monitor, correlate and respond to event logs and security-relevant telemetry from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.                                                                                                                                                                                          | 5                        | Updated 2026.3 | MON-01.4     |
| 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 Event Logs & Security-Relevant Telemetry             | MON-05   | Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.                                                                                                                                                                                                                                      | 5                        |                | MON-02       |
| 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   | Automated Tools for Real Time Event Log & Security-Relevant Telemetry Analysis | MON-05.4 | Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time event log and security-relevant telemetry analysis and incident escalation.                                                                                                                                                                                                                     | 8                        | Updated 2026.3 | MON-01.2     |
| 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-08   | Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.                                                                                                                                                                                 | 5                        |                | MON-02.1     |
| 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-02   | Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.                                                                                                                                                                                                                                       | 5                        |                | IRO-01       |
| 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-06   | Mechanisms exist to cover:<br>(1) Preparation;<br>(2) Automated event detection or manual incident report intake;<br>(3) Analysis;<br>(4) Containment;<br>(5) Eradication; and<br>(6) Recovery.                                                                                                                                                                                                                            | 5                        |                | IRO-02       |
| 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-08   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.                                                                                                                                                                                                                                                                                                     | 5                        |                | IRO-04       |
| 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 Capabilities Testing                                         | IRO-09   | Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.                                                                                                                                                                                                                                                             | 5                        |                | IRO-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 Reporting Assistance                                                  | IRO-18   | 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.                                                                                                                                                                                 | 5                        |                | IRO-11       |
| 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-22   | Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.                                                                                                                                                                                                                 | 5                        |                | IRO-04.1     |
| 8.1   | Coordinated Response            | Respond to incidents in a coordinated and structured manner to ensure the appropriate steps are taken to identify and respond to potential incidents.                                                                                             | Functional     | Intersects With   | Incident Handling                                                              | IRO-06   | Mechanisms exist to cover:<br>(1) Preparation;<br>(2) Automated event detection or manual incident report intake;<br>(3) Analysis;<br>(4) Containment;<br>(5) Eradication; and<br>(6) Recovery.                                                                                                                                                                                                                            | 5                        |                | IRO-02       |
| 8.1   | Coordinated Response            | Respond to incidents in a coordinated and structured manner to ensure the appropriate steps are taken to identify and respond to potential incidents.                                                                                             | Functional     | Intersects With   | Integrated Security Incident Response Team (SIIRT)                             | IRO-11   | Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.                                                                                                                                                                                                                 | 5                        |                | IRO-07       |
| 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-16   | Mechanisms exist to timely-report incidents to applicable:<br>(1) Internal stakeholders;<br>(2) Affected clients & third-parties; and<br>(3) Regulatory authorities.                                                                                                                                                                                                                                                       | 5                        |                | IRO-10       |
| 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-19.1 | Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.                                                                                                                                                                                                                                                                   | 5                        |                | IRO-11.2     |
| 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-02   | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with:<br>(1) The organization's Enterprise Risk Management (ERM); and<br>(2) Industry-recognized cybersecurity risk management practices.                                                                                                                                               | 5                        |                | RSK-01       |
| 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-18   | Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.                                                                                                                                                                                                              | 5                        |                | RSK-06.2     |
| 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 Monitoring                                                                | RSK-22   | Mechanisms exist to monitor risk as an integral part of the continuous monitoring strategy, including:<br>(1) The effectiveness of security, compliance and resilience controls;<br>(2) Changes to the organization's risk profile; and<br>(3) Changes to Technology Assets, Applications and/or Services (TAAS) that affect risk.                                                                                         | 5                        |                | RSK-11       |
| 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-13   | Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).                                                                                                                                      | 5                        |                | RSK-04       |
| 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-13.1 | Mechanisms exist to define instances that require a risk assessment to be performed.                                                                                                                                                                                                                                                                                                                                       | 5                        |                | RSK-04.3     |
| 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-13.3 | Mechanisms exist to:<br>(1) Define applicable stakeholders for each risk assessment;<br>(2) Involve identified stakeholders in the risk assessment process; and<br>(3) Provide identified stakeholders with results of the risk assessment upon completion.                                                                                                                                                                | 5                        |                | RSK-04.4     |
| 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.                                                                                                                                                                                                                                                                                             | 5                        |                | RSK-08       |
| 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-20   | Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.                                                                                                             | 5                        |                | RSK-09       |
| 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 (SCRA)                                            | RSK-21   | Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).                                                                                                                                                                                                                                                                                         | 5                        |                | RSK-09.1     |

| 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 | Legacy SCF # |
|-------|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------|---------------------------------------------------------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|-------|--------------|
| 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-12   | 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) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary). | 5                        |       | IAO-05       |
| 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-14   | Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 5                        |       | RSK-04.1     |
| 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-22   | Mechanisms exist to monitor risk as an integral part of the continuous monitoring strategy, including: (1) The effectiveness of security, compliance and resilience controls; (2) Changes to the organization's risk profile; and (3) Changes to Technology Assets, Applications and/or Services (TAAS) that affect risk.                                                                                                                                                                                                                                                                                                                                                                                                | 5                        |       | RSK-11       |
| 9.4   | Risk Response                             | Responses to identified risks are appropriately identified, categorized and prioritized.                                                                                                                                                                                                               | Functional     | Intersects With   | Risk Response                                                             | RSK-16   | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 5                        |       | RSK-06.1     |
| 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-19   | Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 5                        |       | RSK-10       |
| 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-02   | Mechanisms exist to facilitate the implementation of third-party management controls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 5                        |       | TPM-01       |
| 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-12   | Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 5                        |       | TPM-04       |
| 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-15   | 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                        |       | TPM-08       |
| 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-17   | Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 5                        |       | TPM-10       |
| 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-18   | Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 5                        |       | TPM-09       |
| 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-04   | Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.                                                                                                                                                                                                                                                                                                                                                                                                                                        | 5                        |       | TPM-03       |
| 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-12   | Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 5                        |       | TPM-04       |
| 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-16   | Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 5                        |       | PRI-07       |
| 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-14   | 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                        |       | PRI-07.1     |
| 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-14   | 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                        |       | TPM-05       |
| 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-14.1 | Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 5                        |       | TPM-05.2     |
| 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-11   | Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 5                        |       | PRI-08       |
| 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-11   | Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).                                                                                                                                                                                                                                                                                                                                                                                                                           | 5                        |       | TPM-05.4     |
| 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-12   | Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 5                        |       | TPM-04       |
| 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-15   | 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                        |       | TPM-08       |
| 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-16   | 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 assignments accurately reflect current: (1) Contractual obligations for the External Service Provider (ESP); (2) Business practices; (3) Applicable stakeholders; and (4) Deployed Technology Assets, Applications and/or Services (TAAS).                                                                                                                                                                                                                                                            | 5                        |       | TPM-05.5     |
| 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-17   | Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 5                        |       | TPM-10       |
| 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-18   | Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 5                        |       | TPM-09       |

| 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 | Legacy SCF # |
|-------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------|------------------------------------------------------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|-------|--------------|
| 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-05   | Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRPI) and document all exceptions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 5                        |       | PRM-02       |
| 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-02   | Mechanisms exist to facilitate the implementation of third-party management controls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 5                        |       | TPM-01       |
| 11.1  | Data Privacy Protections Context   | Identify and document the organization's role as a controller and/or processor of sensitive/regulate data, including instances involving more than one party.                                                                                                                             | Functional     | Intersects With   | Defining Business Context & Mission                                          | GOV-06   | Mechanisms exist to document the organization's business model and mission.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 5                        |       | GOV-08       |
| 11.1  | Data Privacy Protections Context   | Identify and document the organization's role as a controller and/or processor of sensitive/regulate data, including instances involving more than one party.                                                                                                                             | Functional     | Intersects With   | Joint Processing of Personal Data (PD)                                       | PRI-43   | Mechanisms exist to clearly define and communicate the organization's role in processing Personal Data (PD) in the data processing ecosystem.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 5                        |       | PRI-07.2     |
| 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-04   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 5                        |       | GOV-02       |
| 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-20   | Mechanisms exist to:<br>(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;<br>(2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories;<br>(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<br>(4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.<br>Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements. | 5                        |       | PRI-01.3     |
| 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   | Conformity Monitoring                                                        | CPL-05   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 5                        |       | CPL-03       |
| 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-04.1 | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRPI), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 5                        |       | GOV-03       |
| 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   | Executive Leadership Oversight of Security, Compliance & Resilience Controls | CPL-07   | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 5                        |       | CPL-02       |
| 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                                                        | DCH-33.1 | Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 5                        |       | PRI-13       |
| 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-09.1 | Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRPI).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 5                        |       | GOV-01.2     |
| 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-12   | Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRPI) measures of performance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 5                        |       | GOV-05       |
| 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-05   | 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                        |       | PRI-14       |
| 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-02   | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 5                        |       | CPL-01       |
| 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-03   | 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                        |       | CPL-01.2     |
| 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-04   | 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                        |       | CPL-01.3     |
| 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-04.1 | 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                        |       | CPL-01.4     |
| 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-Conformity Oversight                                                     | CPL-06   | Mechanisms exist to identify and document instances of non-conformity with statutory, regulatory and/or contractual obligations, in order to develop appropriate risk mitigation actions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 5                        |       | CPL-01.1     |
| 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 & Security-Relevant Telemetry Retention                            | MON-13   | Mechanisms exist to retain event logs and security-relevant telemetry 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                        |       | MON-10       |
| 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-20.2 | Mechanisms exist to review all Privacy Act exemptions claimed for the System of Records Notices (SORN) to ensure they remain appropriate and accurate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 5                        |       | PRI-02.6     |
| 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   | System of Records Notice (SORN)                                              | PRI-20.3 | Mechanisms exist to draft, publish and keep System of Records Notices (SORN) updated in accordance with regulatory guidance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 5                        |       | PRI-02.4     |
| 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-20.4 | 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                        |       | PRI-02.5     |
| 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-20.5 | Mechanisms exist to publish Computer Matching Agreements (CMA) on the organization's public website(s).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 5                        |       | PRI-02.3     |
| 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                                                     | AST-05   | Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 5                        |       | BCD-02       |
| 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 During Development                                      | TDA-05.1 | 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                        |       | TDA-06.1     |
| 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-09   | 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                        |       | TPM-02       |
| 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-09.1 | Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRPI).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 5                        |       | GOV-01.2     |