

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

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

**Focal Document:**

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

**Massachusetts 201 CMR 17.00 (2008)**

<https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the-commonwealth/download>  
<https://content.securecontrolsframework.com/strm/scf-strm-usa-state-ma-201-cmr-17-2008.pdf>

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
17.01	Purpose and Scope	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
17.02	Definitions	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
17.03	Duty to Protect and Standards for Protecting Personal Information	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
17.03(1)	Duty to Protect and Standards for Protecting Personal Information	Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to: The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.	Functional	Subset Of	Security, Compliance & Resilience Program (SCR)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
17.03(1)	Duty to Protect and Standards for Protecting Personal Information	Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to: The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
17.03(1)(a)	Duty to Protect and Standards for Protecting Personal Information	the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program;	Functional	Subset Of	Security, Compliance & Resilience Program (SCR)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
17.03(1)(b)	Duty to Protect and Standards for Protecting Personal Information	the amount of resources available to such person;	Functional	Subset Of	Security, Compliance & Resilience Program (SCR)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
17.03(1)(c)	Duty to Protect and Standards for Protecting Personal Information	the amount of stored data; and	Functional	Subset Of	Security, Compliance & Resilience Program (SCR)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
17.03(1)(d)	Duty to Protect and Standards for Protecting Personal Information	the need for security and confidentiality of both consumer and employee information.	Functional	Subset Of	Security, Compliance & Resilience Program (SCR)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
17.03(2)	Duty to Protect and Standards for Protecting Personal Information	Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:	Functional	Subset Of	Security, Compliance & Resilience Program (SCR)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
17.03(2)(a)	Duty to Protect and Standards for Protecting Personal Information	Designating one or more employees to maintain the comprehensive information security program;	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCR).	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are:1) Implemented correctly, and2) Operating as intended.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications, Services and/or Data (TAASD) under their control on an ongoing basis for applicable threats and risks, as well as to ensure security, compliance and resilience controls are operating as intended.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify:1) Assumptions affecting risk assessments, risk response and risk monitoring;2) Constraints affecting risk assessments, risk response and risk monitoring;3) The organizational risk tolerance; and4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that:1) Document the security categorization results (including supporting rationale) in the security plan for systems; and2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that include 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	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Risk Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
17.03(2)(b)	Duty to Protect and Standards for Protecting Personal Information	Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:	Functional	Intersects With	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5	
17.03(2)(b)1	Duty to Protect and Standards for Protecting Personal Information	ongoing employee (including temporary and contract employee) training;	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
17.03(2)(b)2	Duty to Protect and Standards for Protecting Personal Information	employee compliance with policies and procedures; and	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
17.03(2)(b)2	Duty to Protect and Standards for Protecting Personal Information	employee compliance with policies and procedures; and	Functional	Intersects With	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions:1) Onboarding new personnel (e.g., new hires);2) Transferring personnel into new roles within the organization; and3) Offboarding personnel (e.g., termination of employment).	5	
17.03(2)(b)2	Duty to Protect and Standards for Protecting Personal Information	employee compliance with policies and procedures; and	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
17.03(2)(b)2	Duty to Protect and Standards for Protecting Personal Information	employee compliance with policies and procedures; and	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
17.032(b)3	Duty to Protect and Standards for Protecting Personal Information	means for detecting and preventing security system failures.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
17.032(b)3	Duty to Protect and Standards for Protecting Personal Information	means for detecting and preventing security system failures.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
17.032(c)	Duty to Protect and Standards for Protecting Personal Information	Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
17.032(d)	Duty to Protect and Standards for Protecting Personal Information	Imposing disciplinary measures for violations of the comprehensive information security program rules.	Functional	Subset Of	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	10	
17.032(e)	Duty to Protect and Standards for Protecting Personal Information	Preventing terminated employees from accessing records containing personal information.	Functional	Subset Of	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	10	
17.032(e)	Duty to Protect and Standards for Protecting Personal Information	Preventing terminated employees from accessing records containing personal information.	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	8	
17.032(f)	Duty to Protect and Standards for Protecting Personal Information	Oversee service providers, by:	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
17.032(f)1	Duty to Protect and Standards for Protecting Personal Information	Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with 201 CMR 17.00 and any applicable federal regulations; and	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	8	
17.032(f)2	Duty to Protect and Standards for Protecting Personal Information	Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 201 CMR 17.032(f)2, even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
17.032(g)	Duty to Protect and Standards for Protecting Personal Information	Reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.	Functional	Subset Of	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	10	
17.032(g)	Duty to Protect and Standards for Protecting Personal Information	Reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	8	
17.032(h)	Duty to Protect and Standards for Protecting Personal Information	Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.	Functional	Subset Of	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	10	
17.032(i)	Duty to Protect and Standards for Protecting Personal Information	Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.	Functional	Subset Of	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	10	
17.032(j)	Duty to Protect and Standards for Protecting Personal Information	Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.	Functional	Intersects With	Incident Tracking Repository	IRO-09.3	Mechanisms exist to maintain a repository where cybersecurity events and incidents document: (1) Details of the incident (e.g., category, severity, affected parties, etc.); (2) Remediation actions taken through incident closure; and (3) A summary from the Root Cause Analysis (RCA), if applicable.	5	
17.032(j)	Duty to Protect and Standards for Protecting Personal Information	Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
17.04	Computer System Security Requirements	Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
17.04(1)	Computer System Security Requirements	Secure user authentication protocols including:	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
17.04(1)	Computer System Security Requirements	Secure user authentication protocols including:	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	8	
17.04(1)(a)	Computer System Security Requirements	control of user IDs and other identifiers;	Functional	Subset Of	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	10	
17.04(1)(b)	Computer System Security Requirements	a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;	Functional	Subset Of	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
17.04(1)(c)	Computer System Security Requirements	control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
17.04(1)(d)	Computer System Security Requirements	restricting access to active users and active user accounts only; and	Functional	Subset Of	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	10	
17.04(1)(e)	Computer System Security Requirements	blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;	Functional	Intersects With	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	5	
17.04(2)	Computer System Security Requirements	Secure access control measures that:	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
17.04(2)(a)	Computer System Security Requirements	restrict access to records and files containing personal information to those who need such information to perform their job duties; and	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
17.04(2)(a)	Computer System Security Requirements	restrict access to records and files containing personal information to those who need such information to perform their job duties; and	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	8	
17.04(2)(b)	Computer System Security Requirements	assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	8	
17.04(2)(b)	Computer System Security Requirements	assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	8	
17.04(2)(b)	Computer System Security Requirements	assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
17.04(3)	Computer System Security Requirements	Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.04(3)	Computer System Security Requirements	Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
17.04(4)	Computer System Security Requirements	Reasonable monitoring of systems, for unauthorized use of or access to personal information;	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	8	
17.04(5)	Computer System Security Requirements	Encryption of all personal information stored on laptops or other portable devices;	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
17.04(5)	Computer System Security Requirements	Encryption of all personal information stored on laptops or other portable devices;	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	8	
17.04(6)	Computer System Security Requirements	For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.	Functional	Subset Of	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	10	
17.04(7)	Computer System Security Requirements	Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.	Functional	Intersects With	Stable Versions	VPM-04.1	Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems.	5	
17.04(7)	Computer System Security Requirements	Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	8	
17.04(8)	Computer System Security Requirements	Education and training of employees on the proper use of the computer security system and the importance of personal information security.	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
17.04(8)	Computer System Security Requirements	Education and training of employees on the proper use of the computer security system and the importance of personal information security.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	8	
17.05	Compliance Deadline	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control