Set Theory Relationship Mapping (STRM)

Reference Document : Secure Controls Framework (SCF) version 2024.3
Focal Document: NY DFS 23 NYCRR500 (December 2023 - AMMENDMENT 2)
Focal Document URL: https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf
STRM URL: https://securecontrolsframework.com/content/strm/scf-2024-3-ny-dfs-23-nycrr500-amd2.pdf

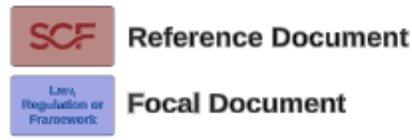
Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

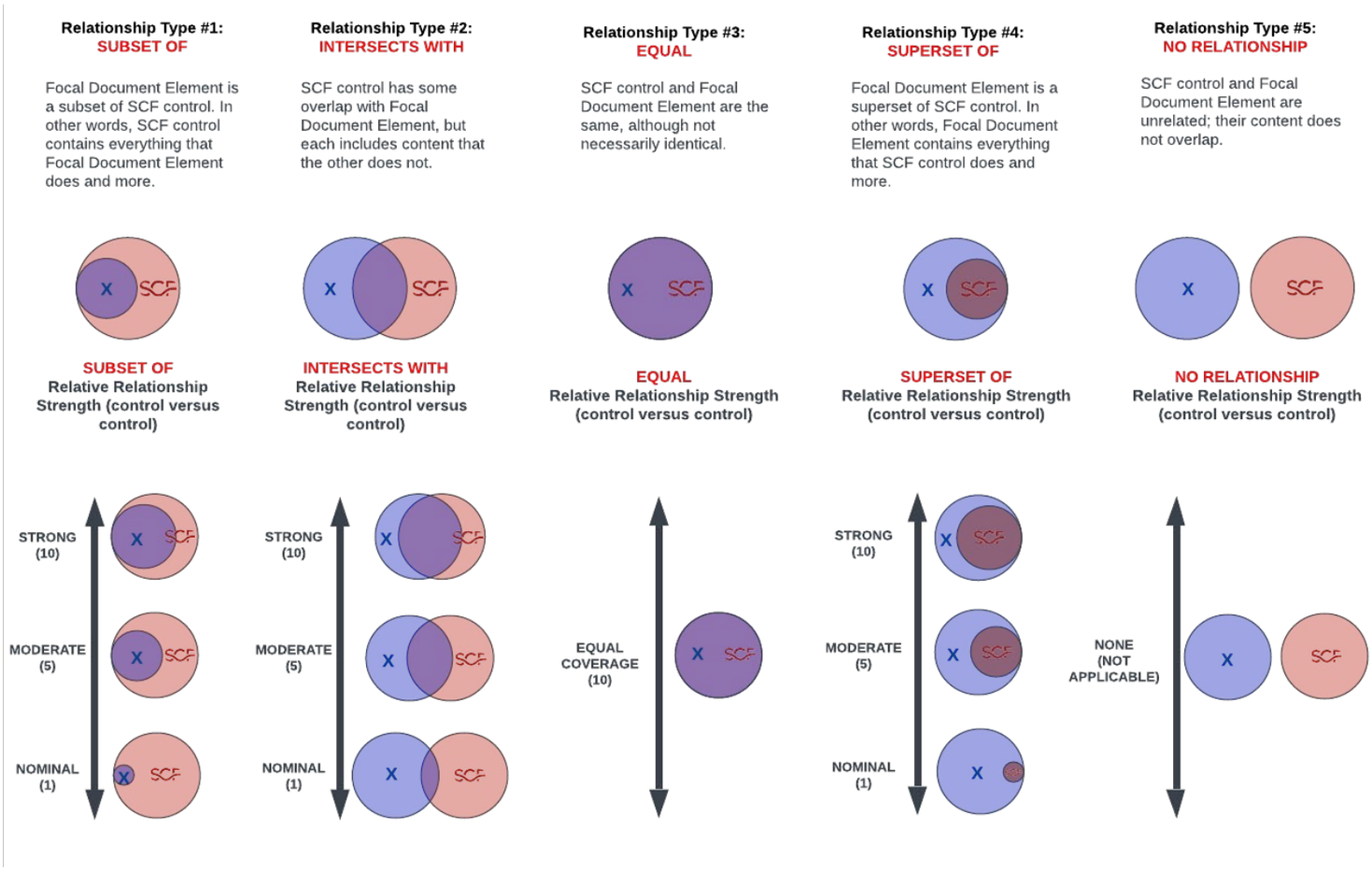
STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two concepts are related:

1. **Syntactic**: How similar is the wording that expresses the two concepts? This is a word-for-word analysis of the relationship, not an interpretation of the language.
2. **Semantic**: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
3. **Functional**: How similar are the results of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed.

Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two distinct concepts:

1. **Subset Of**
2. **Intersects With**
3. **Equal**
4. **Superset Of**
5. **No Relationship**





FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
500.1	Definitions	[see full text of 23 NYCRR 500 for definitions]	Functional	intersects with	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5	
500.2	Cybersecurity Program	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.2(a)	N/A	Each covered entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the covered entity's information systems and nonpublic information stored on those information systems.	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
500.2(b)	N/A	The cybersecurity program shall be based on the covered entity's risk assessment and designed to perform the following core cybersecurity functions:	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
500.2(b)(1)	N/A	identify and assess internal and external cybersecurity risks that may threaten the security or integrity of nonpublic information stored on the covered entity's information systems;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
			Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
			Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
			Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
500.2(b)(2)	N/A	use defensive infrastructure and the implementation of policies and procedures to protect the covered entity's information systems, and the nonpublic information stored on those information systems, from unauthorized access, use or other malicious acts;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
			Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
			Functional	subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
			Functional	subset of	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
			Functional	intersects with	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	
500.2(b)(3)	N/A	detect cybersecurity events;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
			Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
500.2(b)(4)	N/A	respond to identified or detected cybersecurity events to mitigate any negative effects;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
			Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
500.2(b)(5)	N/A	recover from cybersecurity events and restore normal operations and services; and	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
			Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
500.2(b)(6)	N/A	fulfill applicable regulatory reporting obligations.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
			Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
500.2(c)	N/A	Each class A company shall design and conduct independent audits of its cybersecurity program based on its risk assessment.	Functional	subset of	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	10	
			Functional	subset of	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate cybersecurity & data protection controls at planned intervals or when the system, service or project undergoes significant changes.	10	
500.2(d)	N/A	A covered entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the covered entity.	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
			Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
			Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
			Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
			Functional	intersects with	Outsourcing Non-Essential Functions or Services	SEA-02.2	Mechanisms exist to identify non-essential functions or services that are capable of being outsourced to external service providers and align with the organization's enterprise architecture and security standards.	5	
500.2(e)	N/A	All documentation and information relevant to the covered entity's cybersecurity program, including the relevant and applicable provisions of a cybersecurity program maintained by an affiliate and adopted by the covered entity, shall be made available to the superintendent upon request.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
			Functional	intersects with	Legal Assessment of Investigative Inquires	CPL-05	Mechanisms exist to determine whether a government agency has an applicable and valid legal basis to request data from the organization and what further steps need to be taken, if necessary.	5	
			Functional	intersects with	Investigation Access Restrictions	CPL-05.2	Mechanisms exist to support official investigations by provisioning government investigators with "least privileges" and "least functionality" to ensure that government investigators only have access to the data and systems needed to perform the investigation.	5	
			Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
500.3	Cybersecurity Policy	Each covered entity shall implement and maintain a written policy or policies, approved at least annually by a senior officer or the covered entity's senior governing body for the protection of its information systems and nonpublic information stored on those information systems. Procedures shall be developed, documented and implemented in accordance with the written policy or policies. The cybersecurity policy or policies and procedures shall be based on the covered entity's risk assessment and address, at a minimum, the following areas to the extent applicable to the covered entity's operations:	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	8	
			Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	8	
500.3(a)	N/A	information security;	Functional	intersects with	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
			Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
500.3(b)	N/A	data governance, classification and retention;	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
			Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
500.3(c)	N/A	asset inventory, device management and end of life management;	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
			Functional	intersects with	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
500.3(d)	N/A	access controls, including remote access and identity management;	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
			Functional	intersects with	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
500.3(e)	N/A	business continuity and disaster recovery planning and resources;	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
			Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
500.3(f)	N/A	systems operations and availability concerns;	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
			Functional	intersects with	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5	
500.3(g)	N/A	systems and network security and monitoring;	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
			Functional	intersects with	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
500.3(h)	N/A	security awareness and training;	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
			Functional	intersects with	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
500.3(i)	N/A	systems and application security and development and quality assurance;	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
			Functional	intersects with	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
500.3(j)	N/A	physical security and environmental controls;	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
			Functional	intersects with	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
500.3(k)	N/A	customer data privacy;	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
			Functional	intersects with	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data privacy controls.	5	
500.3(l)	N/A	vendor and third-party service provider management;	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
			Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
500.3(m)	N/A	risk assessment;	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
			Functional	intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
500.3(n)	N/A	incident response and notification; and	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
			Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	5	
500.3(o)	N/A	vulnerability management.	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
			Functional	intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
500.4	Chief Information Security Officer.	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.4(a)	N/A	Chief Information Security Officer. Each covered entity shall designate a CISO. The CISO may be employed by the covered entity, one of its affiliates or a third-party service provider. If the CISO is employed by a third-party service provider or an affiliate, the covered entity shall:	Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
500.4(a)(1)	N/A	retain responsibility for compliance with this Part;	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
			Functional	intersects with	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected systems, applications and/or services that the organization utilizes.	5	
			Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
500.4(a)(2)	N/A	designate a senior member of the covered entity's personnel responsible for direction and oversight of the third-party service provider; and	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
			Functional	intersects with	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected systems, applications and/or services that the organization utilizes.	5	
			Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
500.4(a)(3)	N/A	require the third-party service provider or affiliate to maintain a cybersecurity program that protects the covered entity in accordance with the requirements of this Part.	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
			Functional	intersects with	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected systems, applications and/or services that the organization utilizes.	5	
			Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
500.4(b)	N/A	Report. The CISO of each covered entity shall report in writing at least annually to the senior governing bod on the covered entity's cybersecurity program, including to the extent applicable:	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
			Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
			Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	
			Functional	intersects with	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
			Functional	intersects with	Materiality Determination	GOV-16	Mechanisms exist to define materiality threshold criteria capable of designating an incident as material to the organization.	5	
			Functional	intersects with	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5	
			Functional	intersects with	Material Threats	GOV-16.2	Mechanisms exist to define criteria necessary to designate a threat as a material threat.	5	
500.4(b)(1)	N/A	the confidentiality of nonpublic information and the integrity and security of the covered entity's information systems;	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
			Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity & data privacy controls, including any flow-down requirements to subcontractors.	5	
500.4(b)(2)	N/A	the covered entity's cybersecurity policies and procedures;	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
			Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity & data privacy controls, including any flow-down requirements to subcontractors.	5	
500.4(b)(3)	N/A	material cybersecurity risks to the covered entity;	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
			Functional	intersects with	Materiality Determination	GOV-16	Mechanisms exist to define materiality threshold criteria capable of designating an incident as material to the organization.	5	
			Functional	intersects with	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5	
			Functional	intersects with	Material Threats	GOV-16.2	Mechanisms exist to define criteria necessary to designate a threat as a material threat.	5	
			Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity & data privacy controls, including any flow-down requirements to subcontractors.	5	
500.4(b)(4)	N/A	overall effectiveness of the covered entity's cybersecurity program;	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
			Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity & data privacy controls, including any flow-down requirements to subcontractors.	5	
500.4(b)(5)	N/A	material cybersecurity events involving the covered entity during the time period addressed by the report; and	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
			Functional	intersects with	Materiality Determination	GOV-16	Mechanisms exist to define materiality threshold criteria capable of designating an incident as material to the organization.	5	
			Functional	intersects with	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5	
			Functional	intersects with	Material Threats	GOV-16.2	Mechanisms exist to define criteria necessary to designate a threat as a material threat.	5	
			Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity & data privacy controls, including any flow-down requirements to subcontractors.	5	
500.4(b)(6)	N/A	plans for remediating material inadequacies.	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
			Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	
			Functional	intersects with	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
			Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
			Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
			Functional	intersects with	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
500.4(c)	N/A	The CISO shall timely report to the senior governing body or senior officer(s) on material cybersecurity issues, such as significant cybersecurity events and significant changes to the covered entity's cybersecurity program.	Functional	subset of	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	10	
500.4(d)	N/A	The senior governing body of the covered entity shall exercise oversight of the covered entity's cybersecurity risk management, including by:	Functional	subset of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	10	
500.4(d)(1)	N/A	having sufficient understanding of cybersecurity-related matters to exercise such oversight, which may include the use of advisors;	Functional	subset of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	10	
500.4(d)(2)	N/A	requiring the covered entity's executive management or its designees to develop, implement and maintain the covered entity's cybersecurity program;	Functional	subset of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	10	
500.4(d)(3)	N/A	regularly receiving and reviewing management reports about cybersecurity matters; and	Functional	subset of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	10	
500.4(d)(4)	N/A	confirming that the covered entity's management has allocated sufficient resources to implement and maintain an effective cybersecurity program.	Functional	subset of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	10	
			Functional	subset of	Cybersecurity & Data Privacy Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity & data privacy programs and document all exceptions to this requirement.	10	
			Functional	intersects with	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.	5	
500.5	Vulnerability Management	Each covered entity shall, in accordance with its risk assessment, develop and implement written policies and procedures for vulnerability management that are designed to assess and maintain the effectiveness of its cybersecurity program. These policies and procedures shall be designed to ensure that covered entities:	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
500.5(a)	N/A	conduct, at a minimum:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.5(a)(1)	N/A	penetration testing of their information systems from both inside and outside the information systems' boundaries by a qualified internal or external party at least annually; and	Functional	intersects with	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
			Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	8	
500.5(a)(2)	N/A	automated scans of information systems, and a manual review of systems not covered by such scans, for the purpose of discovering, analyzing and reporting vulnerabilities at a frequency determined by the risk assessment, and promptly after any material system changes;	Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	
500.5(b)	N/A	are promptly informed of new security vulnerabilities by having a monitoring process in place; and	Functional	intersects with	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	
500.5(c)	N/A	timely remediate vulnerabilities, giving priority to vulnerabilities based on the risk they pose to the covered entity.	Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
			Functional	intersects with	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	
			Functional	intersects with	Vulnerability Exploitation Analysis	VPM-03.1	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.	5	
500.6	Audit Trail	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.6(a)	N/A	Each covered entity shall securely maintain systems that, to the extent applicable and based on its risk assessment:	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
500.6(a)(1)	N/A	are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the covered entity; and	Functional	intersects with	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
			Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: ▪ Establish what type of event occurred; ▪ When (date and time) the event occurred; ▪ Where the event occurred; ▪ The source of the event; ▪ The outcome (success or failure) of the event; and ▪ The identity of any user/subject associated with the event.	5	
500.6(a)(2)	N/A	include audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the covered entity.	Functional	intersects with	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
			Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
			Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: ▪ Establish what type of event occurred; ▪ When (date and time) the event occurred; ▪ Where the event occurred; ▪ The source of the event; ▪ The outcome (success or failure) of the event; and ▪ The identity of any user/subject associated with the event.	5	
500.6(b)	N/A	Each covered entity shall maintain records required by paragraph (a)(1) of this section for not fewer than five years and shall maintain records required by paragraph (a)(2) of this section for not fewer than three years.	Functional	intersects with	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
			Functional	intersects with	Retain Access Records	IAC-01.1	Mechanisms exist to retain a record of personnel accountability to ensure there is a record of all access granted to an individual (system and application-wise), who provided the authorization, when the authorization was granted and when the access was last reviewed.	5	
			Functional	intersects with	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5	
500.7	Access Privileges	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.7(a)	N/A	As part of its cybersecurity program, based on the covered entity's risk assessment each covered entity shall:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.7(a)(1)	N/A	limit user access privileges to information systems that provide access to nonpublic information to only those necessary to perform the user's job;	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
			Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
			Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	
			Functional	intersects with	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	
			Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
			Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
500.7(a)(2)	N/A	limit the number of privileged accounts and limit the access functions of privileged accounts to only those necessary to perform the user's job;	Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
500.7(a)(3)	N/A	limit the use of privileged accounts to only when performing functions requiring the use of such access;	Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	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 (optional)	Notes (optional)
500.7(a)(4)	N/A	periodically, but at a minimum annually, review all user access privileges and remove or disable accounts and access that are no longer necessary;	Functional	intersects with	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	5	
			Functional	intersects with	System Account Reviews	IAC-15.7	Mechanisms exist to review all system accounts and disable any account that cannot be associated with a business process and owner.	5	
			Functional	intersects with	Privileged Account Inventories	IAC-16.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	5	
500.7(a)(5)	N/A	disable or securely configure all protocols that permit remote control of devices; and	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
			Functional	intersects with	Use of Privileged Utility Programs	IAC-20.3	Mechanisms exist to restrict and tightly control utility programs that are capable of overriding system and application controls.	5	
500.7(a)(6)	N/A	promptly terminate access following departures.	Functional	intersects with	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to systems and facilities upon personnel reassignment or transfer, in a timely manner.	5	
			Functional	intersects with	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
500.7(b)	N/A	To the extent passwords are employed as a method of authentication, the covered entity shall implement a written password policy that meets industry standards.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	intersects with	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
			Functional	intersects with	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	
			Functional	intersects with	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
500.7(c)	N/A	Each class A company shall monitor privileged access activity and shall implement:	Functional	intersects with	Privileged User Oversight	MON-01.15	Mechanisms exist to implement enhanced activity monitoring for privileged users.	5	
			Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: ▪ Establish what type of event occurred; ▪ When (date and time) the event occurred; ▪ Where the event occurred; ▪ The source of the event; ▪ The outcome (success or failure) of the event; and ▪ The identity of any user/subject associated with the event.	5	
			Functional	intersects with	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	5	
500.7(c)(1)	N/A	a privileged access management solution; and	Functional	equal	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	10	
500.7(c)(2)	N/A	an automated method of blocking commonly used passwords for all accounts on information systems owned or controlled by the class A company and wherever feasible for all other accounts. To the extent the class A company determines that blocking commonly used passwords is infeasible, the covered entity's CISO may instead approve in writing at least annually the infeasibility and the use of reasonably equivalent or more secure compensating controls.	Functional	intersects with	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
			Functional	intersects with	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5	
500.8	Application Security	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.8(a)	N/A	Each covered entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the covered entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the covered entity within the context of the covered entity's technology environment.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
			Functional	subset of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
			Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
			Functional	intersects with	Software Design Review	TDA-06.5	Mechanisms exist to have an independent review of the software design to confirm that all cybersecurity & data privacy requirements are met and that any identified risks are satisfactorily addressed.	5	
			Functional	intersects with	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy personnel to: ▪ Create and implement a Security Test and Evaluation (ST&E) plan; ▪ Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and ▪ Document the results of the security testing/evaluation and flaw remediation processes.	5	
			Functional	intersects with	Secure Settings By Default	TDA-09.6	Mechanisms exist to implement secure configuration settings by default to reduce the likelihood of software being deployed with weak security settings that would put the asset at a greater risk of compromise.	5	
500.8(b)	N/A	All such procedures, guidelines and standards shall be reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the covered entity at least annually.	Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
500.9	Risk Assessment	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
		Each covered entity shall conduct a periodic risk assessment of the covered entity's information systems sufficient to inform the design of the cybersecurity program as required by this Part. Such risk assessment shall be reviewed and updated as reasonably necessary, but at a minimum annually, and whenever a change in the business or technology causes a material change to the covered entity's cyber risk. The covered entity's risk	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
500.9(a)	N/A	assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the covered entity's business operations related to cybersecurity, nonpublic information collected or stored, information systems utilized and the availability and effectiveness of controls to protect nonpublic information and information systems.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
			Functional	intersects with	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
			Functional	intersects with	Risk Assessment Update	RSK-07	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	5	
500.9(b)	N/A	The risk assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
			Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
500.9(b)(1)	N/A	criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the covered entity;	Functional	intersects with	Materiality Determination	GOV-16	Mechanisms exist to define materiality threshold criteria capable of designating an incident as material to the organization.	5	
			Functional	intersects with	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5	
			Functional	intersects with	Material Threats	GOV-16.2	Mechanisms exist to define criteria necessary to designate a threat as a material threat.	5	
			Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: ▪ Assumptions affecting risk assessments, risk response and risk monitoring; ▪ Constraints affecting risk assessments, risk response and risk monitoring; ▪ The organizational risk tolerance; and ▪ Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
			Functional	intersects with	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
			Functional	intersects with	Risk Threshold	RSK-01.4	Mechanisms exist to define organizational risk threshold, the level of risk exposure above which risks are addressed and below which risks may be accepted.	5	
			Functional	intersects with	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	5	
			Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
			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	
			Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
			Functional	intersects with	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
			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	
			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	
500.9(b)(2)	N/A	criteria for the assessment of the confidentiality, integrity, security and availability of the covered entity's information systems and nonpublic information, including the adequacy of existing controls in the context of identified risks; and	Functional	intersects with	Materiality Determination	GOV-16	Mechanisms exist to define materiality threshold criteria capable of designating an incident as material to the organization.	5	
			Functional	intersects with	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5	
			Functional	intersects with	Material Threats	GOV-16.2	Mechanisms exist to define criteria necessary to designate a threat as a material threat.	5	
			Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
500.9(b)(3)	N/A	requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the cybersecurity program will address the risks.	Functional	intersects with	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	5	
			Functional	intersects with	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize systems and data in accordance with applicable local, state and Federal laws that: ▪ Document the security categorization results (including supporting rationale) in the security plan for systems; and ▪ Ensure the security categorization decision is reviewed and approved by the asset owner.	5	
			Functional	intersects with	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for systems, applications and/or services to prevent potential disruptions.	5	
			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	
			Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
			Functional	intersects with	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	
			Functional	intersects with	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
500.10	Cybersecurity Personnel and Intelligence	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.10(a)	N/A	In addition to the requirements set forth in section 500.4(a) of this Part, each covered entity shall:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
		utilize qualified cybersecurity personnel of the covered entity, an affiliate or a thirdparty service provider sufficient to manage the covered entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 500.2(b)(1)–(6) of this Part;	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
			Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	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 (optional)	Notes (optional)
500.10(a)(1)	N/A		Functional	intersects with	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
			Functional	intersects with	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	
			Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
			Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
			Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
500.10(a)(2)	N/A	provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; 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	
			Functional	intersects with	Formal Indoctrination	HRS-04.2	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information are formally indoctrinated for all the relevant types of information to which they have access on the system.	5	
			Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
			Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
			Functional	intersects with	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: ▪ Before authorizing access to the system or performing assigned duties; ▪ When required by system changes; and ▪ Annually thereafter.	5	
			Functional	intersects with	Sensitive Information Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive information is formally trained in data handling requirements.	5	
			Functional	intersects with	Privileged Users	SAT-03.5	Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities	5	
			Functional	intersects with	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity & data privacy awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
			Functional	intersects with	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	
500.10(a)(3)	N/A	verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.	Functional	intersects with	Continuing Professional Education (CPE) - Cybersecurity & Data Privacy Personnel	SAT-03.7	Mechanisms exist to ensure cybersecurity & data privacy personnel receive Continuing Professional Education (CPE) training to maintain currency and proficiency with industry-recognized secure practices that are pertinent to their assigned roles and responsibilities.	5	
			Functional	intersects with	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	
500.10(b)	N/A	A covered entity may choose to utilize an affiliate or qualified third-party service provider to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in sections 500.4 and 500.11 of this Part.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
			Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
			Functional	intersects with	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
500.11	Third Party Service Provider Security Policy	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.11(a)	N/A	Each covered entity shall implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers. Such policies and procedures shall be based on the risk assessment of the covered entity and shall address to the extent applicable:	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
			Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
500.11(a)(1)	N/A	the identification and risk assessment of third-party service providers;	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
			Functional	intersects with	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
			Functional	intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
			Functional	intersects with	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	5	
			Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
			Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
			Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
500.11(a)(2)	N/A	minimum cybersecurity practices required to be met by such third-party service providers in order for them to do business with the covered entity;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
			Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
500.11(a)(3)	N/A	due diligence processes used to evaluate the adequacy of cybersecurity practices of such third-party service providers; 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 services.	5	
			Functional	intersects with	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity & data privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	
			Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity & data privacy controls, including any flow-down requirements to subcontractors.	5	
			Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
500.11(a)(4)	N/A	periodic assessment of such third-party service providers based on the risk they present and the continued adequacy of their cybersecurity practices.	Functional	intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
			Functional	intersects with	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity & data privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	
			Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
500.11(b)	N/A	Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to third-party service providers including to the extent applicable guidelines addressing:	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
			Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
			Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
500.11(b)(1)	N/A	the third-party service provider's policies and procedures for access controls, including its use of multi-factor authentication as required by section 500.12 of this Part, to limit access to relevant information systems and nonpublic information;	Functional	subset of	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: ▪ Remote network access; ▪ Third-party systems, applications and/or services; and/ or ▪ Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	10	
			Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
			Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
			Functional	intersects with	Third-Party Authentication Practices	TPM-05.3	Mechanisms exist to ensure External Service Providers (ESPs) use unique authentication factors for each of its customers.	5	
500.11(b)(2)	N/A	the third-party service provider's policies and procedures for use of encryption as required by section 500.15 of this Part to protect nonpublic information in transit and at rest;	Functional	intersects with	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
			Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
			Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
500.11(b)(3)	N/A	notice to be provided to the covered entity in the event of a cybersecurity event directly impacting the covered entity's information systems or the covered entity's nonpublic information being held by the third-party service provider; and	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
			Functional	intersects with	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected systems, applications and/or services that the organization utilizes.	5	
			Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
500.11(b)(4)	N/A	representations and warranties addressing the third-party service provider's cybersecurity policies and procedures that relate to the security of the covered entity's information systems or nonpublic information.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
			Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
			Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity & data privacy controls, including any flow-down requirements to subcontractors.	5	
500.12	Multi-Factor Authentication	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.12(a)	N/A	Multi-factor authentication shall be utilized for any individual accessing any information systems of a covered entity, unless the covered entity qualifies for a limited exemption pursuant to section 500.19(a) of this Part in which case multi-factor authentication shall be utilized for:	Functional	intersects with	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: ▪ Remote network access; ▪ Third-party systems, applications and/or services; and/ or ▪ Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	
500.12(a)(1)	N/A	remote access to the covered entity's information systems;	Functional	intersects with	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: ▪ Remote network access; ▪ Third-party systems, applications and/or services; and/ or ▪ Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	
500.12(a)(2)	N/A	remote access to third-party applications, including but not limited to those that are cloud based, from which nonpublic information is accessible; and	Functional	intersects with	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: ▪ Remote network access; ▪ Third-party systems, applications and/or services; and/ or ▪ Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	
500.12(a)(3)	N/A	all privileged accounts other than service accounts that prohibit interactive login.	Functional	intersects with	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
			Functional	intersects with	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	
500.12(b)	N/A	If the covered entity has a CISO, the CISO may approve in writing the use of reasonably equivalent or more secure compensating controls. Such controls shall be reviewed periodically, but at a minimum annually.	Functional	intersects with	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	5	
			Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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 (optional)	Notes (optional)
			Functional	subset of	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	10	
500.13	Asset Management and Data Retention Requirements	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.13(a)	N/A	As part of its cybersecurity program, each covered entity shall implement written policies and procedures designed to produce and maintain a complete, accurate and documented asset inventory of the covered entity's information systems. The asset inventory shall be maintained in accordance with written policies and procedures. At a minimum, such policies and procedures shall include:	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	intersects with	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
			Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and ▪ Is available for review and audit by designated organizational personnel.	5	
500.13(a)(1)	N/A	a method to track key information for each asset, including, as applicable, the following:	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and ▪ Is available for review and audit by designated organizational personnel.	5	
500.13(a)(1)(i)	N/A	owner;	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and ▪ Is available for review and audit by designated organizational personnel.	5	
500.13(a)(1)(ii)	N/A	location;	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and ▪ Is available for review and audit by designated organizational personnel.	5	
500.13(a)(1)(iii)	N/A	classification or sensitivity;	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and ▪ Is available for review and audit by designated organizational personnel.	5	
500.13(a)(1)(iv)	N/A	support expiration date; and	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and ▪ Is available for review and audit by designated organizational personnel.	5	
500.13(a)(1)(v)	N/A	recovery time objectives; and	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and ▪ Is available for review and audit by designated organizational personnel.	5	
500.13(a)(2)	N/A	the frequency required to update and validate the covered entity's asset inventory.	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and ▪ Is available for review and audit by designated organizational personnel.	5	
500.13(b)	N/A	As part of its cybersecurity program, each covered entity shall include policies and procedures for the secure disposal on a periodic basis of any nonpublic information identified in section 500.1(k)(2)–(3) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the covered entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.	Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
			Functional	intersects with	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
500.14	Training and Monitoring	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.14(a)	N/A	As part of its cybersecurity program, each covered entity shall:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.14(a)(1)	N/A	implement risk-based policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, nonpublic information by such authorized users;	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	intersects with	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
			Functional	intersects with	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
500.14(a)(2)	N/A	implement risk-based controls designed to protect against malicious code, including those that monitor and filter web traffic and electronic mail to block malicious content; and	Functional	intersects with	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
			Functional	intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
			Functional	intersects with	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	5	
			Functional	intersects with	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
			Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
500.14(a)(3)	N/A	provide periodic, but at a minimum annual, cybersecurity awareness training that includes social engineering for all personnel that is updated to reflect risks identified by the covered entity in its risk assessment.	Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
500.14(b)	N/A	Each class A company shall implement, unless the CISO has approved in writing the use of reasonably equivalent or more secure compensating controls:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.14(b)(1)	N/A	an endpoint detection and response solution to monitor anomalous activity, including but not limited to lateral movement; and	Functional	intersects with	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
			Functional	intersects with	Endpoing Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	5	
			Functional	intersects with	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor anomalous host activity, including lateral movement across the network.	5	
500.14(b)(2)	N/A	a solution that centralizes logging and security event alerting.	Functional	intersects with	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
			Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
500.15	Encryption of Nonpublic Information	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.15(a)	N/A	As part of its cybersecurity program, each covered entity shall implement a written policy requiring encryption that meets industry standards, to protect nonpublic information held or transmitted by the covered entity both in transit over external networks and at rest.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	intersects with	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
			Functional	intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
			Functional	intersects with	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
500.15(b)	N/A	To the extent a covered entity determines that encryption of nonpublic information at rest is infeasible, the covered entity may instead secure such nonpublic information using effective alternative compensating controls that have been reviewed and approved by the covered entity's CISO in writing. The feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.	Functional	intersects with	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
			Functional	intersects with	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards.	5	
			Functional	intersects with	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	5	
			Functional	intersects with	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
500.16	Incident Response Plan	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.16(a)	N/A	As part of its cybersecurity program, each covered entity shall establish written plans that contain proactive measures to investigate and mitigate cybersecurity events and to ensure operational resilience, including but not limited to incident response, business continuity and disaster recovery plans.	Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	5	
			Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
			Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
500.16(a)(1)	N/A	Incident response plan. Incident response plans shall be reasonably designed to enable prompt response to, and recovery from, any cybersecurity event materially affecting the confidentiality, integrity or availability of the covered entity's information systems or the continuing functionality of any aspect of the covered entity's business or operations. Such plans shall address the following areas with respect to different types of cybersecurity events, including disruptive events such as ransomware incidents:	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	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 (optional)	Notes (optional)
500.16(a)(1)(i)	N/A	the goals of the incident response plan;	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
500.16(a)(1)(ii)	N/A	the internal processes for responding to a cybersecurity event;	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
500.16(a)(1)(iii)	N/A	the definition of clear roles, responsibilities and levels of decision-making authority;	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
500.16(a)(1)(iv)	N/A	external and internal communications and information sharing;	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
500.16(a)(1)(v)	N/A	identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
500.16(a)(1)(vi)	N/A	documentation and reporting regarding cybersecurity events and related incident response activities;	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
500.16(a)(1)(vii)	N/A	recovery from backups;	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
500.16(a)(1)(viii)	N/A	preparation of root cause analysis that describes how and why the event occurred, what business impact it had, and what will be done to prevent reoccurrence; and	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
500.16(a)(1)(ix)	N/A	updating of incident response plans as necessary.	Functional	intersects with	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5	
500.16(a)(2)	N/A	Business continuity and disaster recovery (BCDR) plan. BCDR plans shall be reasonably designed to ensure the availability and functionality of the covered entity's information systems and material services and protect the covered entity's personnel, assets and nonpublic information in the event of a cybersecurity-related disruption to its normal business activities. Such plans shall, at minimum:	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
500.16(a)(2)(i)	N/A	identify documents, data, facilities, infrastructure, services, personnel and competencies essential to the continued operations of the covered entity's business;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
			Functional	intersects with	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical systems, applications and services that support essential missions and business functions.	5	
500.16(a)(2)(ii)	N/A	identify the supervisory personnel responsible for implementing each aspect of the BCDR plan;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
			Functional	intersects with	Recovery Operations Criteria	BCD-01.5	Mechanisms exist to define specific criteria that must be met to initiate Business Continuity / Disaster Recover (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
			Functional	intersects with	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
			Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
500.16(a)(2)(iii)	N/A	include a plan to communicate with essential persons in the event of a cybersecurity-related disruption to the operations of the covered entity, including employees, counterparties, regulatory authorities, third-party service providers, disaster recovery specialists, the senior governing body and any other persons essential to the recovery of documentation and data and the resumption of operations;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
			Functional	intersects with	Recovery Operations Communications	BCD-01.6	Mechanisms exist to communicate the status of recovery activities and progress in restoring operational capabilities to designated internal and external stakeholders.	5	
500.16(a)(2)(iv)	N/A	include procedures for the timely recovery of critical data and information systems and to resume operations as soon as reasonably possible following a cybersecurity-related disruption to normal business activities;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
			Functional	intersects with	Continue Essential Mission & Business Functions	BCD-02.2	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites.	5	
500.16(a)(2)(v)	N/A	include procedures for backing up or copying, with sufficient frequency, information essential to the operations of the covered entity and storing such information offsite; and	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
			Functional	intersects with	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
			Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
500.16(a)(2)(vi)	N/A	identify third parties that are necessary to the continued operations of the covered entity's information systems.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
			Functional	intersects with	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical systems, applications and services that support essential missions and business functions.	5	
500.16(b)	N/A	Each covered entity shall ensure that current copies of the plans or relevant portions therein are distributed or are otherwise accessible, including during a cybersecurity event, to all employees necessary to implement such plans.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
			Functional	subset of	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	
500.16(c)	N/A	Each covered entity shall provide relevant training to all employees responsible for implementing the plans regarding their roles and responsibilities.	Functional	equal	Contingency Training	BCD-03	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	10	
500.16(d)	N/A	Each covered entity shall periodically, but at a minimum annually, test its:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.16(d)(1)	N/A	incident response and BCDR plans with all staff and management critical to the response, and shall revise the plan as necessary; and	Functional	intersects with	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	8	
			Functional	intersects with	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	8	
500.16(d)(2)	N/A	ability to restore its critical data and information systems from backups.	Functional	equal	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	10	
500.16(e)	N/A	Each covered entity shall maintain backups necessary to restore material operations. The backups shall be adequately protected from unauthorized alterations or destruction.	Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
			Functional	intersects with	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	5	
			Functional	intersects with	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
500.17	Notices to Superintendent	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.17(a)	N/A	Notice of cybersecurity incident.	Functional	no relationship	N/A	N/A	N/A	N/A	

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
500.17(a)(1)	N/A	Each covered entity shall notify the superintendent electronically in the form set forth on the department's website as promptly as possible but in no event later than 72 hours after determining that a cybersecurity incident has occurred at the covered entity, its affiliates, or a third-party service provider.	Functional	intersects with	Cybersecurity & Data Privacy Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	5	
			Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: ▪ Internal stakeholders; ▪ Affected clients & third-parties; and ▪ Regulatory authorities.	5	
			Functional	intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
			Functional	intersects with	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	5	
500.17(a)(2)	N/A	Each covered entity shall promptly provide to the superintendent any information requested regarding such incident. Covered entities shall have a continuing obligation to update the superintendent with material changes or new information previously unavailable.	Functional	intersects with	Cybersecurity & Data Privacy Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	5	
			Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
			Functional	intersects with	Legal Assessment of Investigative Inquires	CPL-05	Mechanisms exist to determine whether a government agency has an applicable and valid legal basis to request data from the organization and what further steps need to be taken, if necessary.	5	
			Functional	intersects with	Investigation Access Restrictions	CPL-05.2	Mechanisms exist to support official investigations by provisioning government investigators with "least privileges" and "least functionality" to ensure that government investigators only have access to the data and systems needed to perform the investigation.	5	
500.17(b)	N/A	Notice of compliance.	Functional	no relationship	N/A	N/A	N/A	N/A	
500.17(b)(1)	N/A	Annually each covered entity shall submit to the superintendent electronically by April 15 either:	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
500.17(b)(1)(i)	N/A	a written certification that:	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
500.17(b)(1)(i)(a)	N/A	certifies that the covered entity materially complied with the requirements set forth in this Part during the prior calendar year; and	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
500.17(b)(1)(i)(b)	N/A	shall be based upon data and documentation sufficient to accurately determine and demonstrate such material compliance, including, to the extent necessary, documentation of officers, employees, representatives, outside vendors and other individuals or entities, as well as other documentation, whether in the form of reports, certifications, schedules or otherwise; or	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
500.17(b)(1)(ii)	N/A	a written acknowledgment that:	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
500.17(b)(1)(ii)(a)	N/A	acknowledges that, for the prior calendar year, the covered entity did not materially comply with all the requirements of this Part;	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
500.17(b)(1)(ii)(b)	N/A	identifies all sections of this Part that the entity has not materially complied with and describes the nature and extent of such noncompliance; and	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
500.17(b)(1)(ii)(c)	N/A	provides a remediation timeline or confirmation that remediation has been completed.	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
500.17(b)(2)	N/A	Such certification or acknowledgment shall be submitted electronically in the form set forth on the department's website and shall be signed by the covered entity's highestranking executive and its CISO. If the covered entity does not have a CISO, the certification or acknowledgment shall be signed by the highest-ranking executive and by the senior officer responsible for the cybersecurity program of the covered entity.	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
500.17(b)(3)	N/A	Each covered entity shall maintain for examination and inspection by the department upon request all records, schedules and other documentation and data supporting the certification or acknowledgment for a period of five years, including the identification of all areas, systems and processes that require or required material improvement, updating or redesign, all remedial efforts undertaken to address such areas, systems and processes, and remediation plans and timelines for their implementation.	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
500.17(c)	N/A	Notice and explanation of extortion payment. Each covered entity, in the event of an extortion payment made in connection with a cybersecurity event involving the covered entity, shall provide the superintendent electronically, in the form set forth on the department's website, with the following:	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
			Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: ▪ Internal stakeholders; ▪ Affected clients & third-parties; and ▪ Regulatory authorities.	5	
500.17(c)(1)	N/A	within 24 hours of the extortion payment, notice of the payment; and	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: ▪ Internal stakeholders; ▪ Affected clients & third-parties; and ▪ Regulatory authorities.	5	
500.17(c)(2)	N/A	within 30 days of the extortion payment, a written description of the reasons payment was necessary, a description of alternatives to payment considered, all diligence performed to find alternatives to payment and all diligence performed to ensure compliance with applicable rules and regulations including those of the Office of Foreign Assets Control.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: ▪ Internal stakeholders; ▪ Affected clients & third-parties; and ▪ Regulatory authorities.	5	
500.18	Confidentiality	Information provided by a covered entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable State or Federal law.	Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
			Functional	intersects with	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
500.19	Exemptions	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.19(a)	N/A	Limited exemption. Each covered entity with: ...shall be exempt from the requirements of sections 500.4, 500.5, 500.6, 500.8, 500.10, 500.14(a)(1), (a)(2), and (b), 500.15 and 500.16 of this Part.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.19(a)(1)	N/A	fewer than 20 employees and independent contractors of the covered entity and its affiliates;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.19(a)(2)	N/A	less than $7,500,000 in gross annual revenue in each of the last three fiscal years from all business operations of the covered entity and the business operations in this State of the covered entity's affiliates; or	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.19(a)(3)	N/A	less than $15,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates,	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.19(b)	N/A	An employee, agent, wholly owned subsidiary, representative or designee of a covered entity, who is itself a covered entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, wholly owned subsidiary, representative or designee is covered by the cybersecurity program of the covered entity.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
500.19(c)	N/A	A covered entity that does not directly or indirectly operate, maintain, utilize or control any information systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess nonpublic information shall be exempt from the requirements of sections 500.2, 500.3, 500.4, 500.5, 500.6, 500.7, 500.8, 500.10, 500.12, 500.14, 500.15 and 500.16 of this Part.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.19(d)	N/A	A covered entity under article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess nonpublic information other than information relating to its corporate parent company (or affiliates) shall be exempt from the requirements of sections 500.2, 500.3, 500.4, 500.5, 500.6, 500.7, 500.8, 500.10, 500.12, 500.14, 500.15 and 500.16 of this Part.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.19(e)	N/A	An individual insurance broker subject to Insurance Law section 2104 who qualifies for the exemption pursuant to subdivision 500.19(c) of this Part and has not, for any compensation, commission or other thing of value, acted or aided in any manner in soliciting, negotiating or selling any policy or contract or in placing risks or taking out insurance on behalf of another person for at least one year shall be exempt from the requirements of this Part, provided such individuals do not otherwise qualify as a covered entity for purposes of this Part.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.19(f)	N/A	A covered entity that qualifies for any of the above exemptions pursuant to this section shall file electronically a Notice of Exemption in the form set forth on the department's website within 30 days of the determination that the covered entity is exempt.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.19(g)	N/A	The following persons are exempt from the requirements of this Part, provided such persons do not otherwise qualify as a covered entity for purposes of this Part: persons subject to Insurance Law section 1110; persons subject to Insurance Law section 5904; any accredited reinsurer, certified reinsurer or reciprocal jurisdiction reinsurer that has been so recognized pursuant to 11 NYCRR Part 125; individual insurance agents who are placed in inactive status under Insurance Law section 2103; and individual licensees placed in inactive status under Banking Law section 599-i.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.19(h)	N/A	In the event that a covered entity ceases to qualify for an exemption, such covered entity shall have 180 days from the date that it ceases to so qualify to comply with all applicable requirements of this Part.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20	Enforcement	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(a)	N/A	This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(b)	N/A	The commission of a single act prohibited by this Part or the failure to act to satisfy an obligation required by this Part shall constitute a violation hereof. Such acts or failures include, without limitation:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(b)(1)	N/A	the failure to secure or prevent unauthorized access to an individual's or an entity's nonpublic information due to noncompliance with any section of this Part; or	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(b)(2)	N/A	the material failure to comply for any 24-hour period with any section of this Part.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)	N/A	In assessing any penalty for a violation of this Part pursuant to the Banking Law, Insurance Law or Financial Services Law, the superintendent shall take into account, without limitation, factors including:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(1)	N/A	the extent to which the covered entity has cooperated with the superintendent in the investigation of such acts;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(2)	N/A	the good faith of the entity;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(3)	N/A	whether the violations resulted from conduct that was unintentional or inadvertent, reckless or intentional and deliberate;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(4)	N/A	whether the violation was a result of failure to remedy previous examination matters requiring attention, or failing to adhere to any disciplinary letter, letter of instructions or similar;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(5)	N/A	any history of prior violations;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(6)	N/A	whether the violation involved an isolated incident, repeat violations, systemic violations or a pattern of violations;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(7)	N/A	whether the covered entity provided false or misleading information;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(8)	N/A	the extent of harm to consumers;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(9)	N/A	whether required, accurate and timely disclosures were made to affected consumers;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(10)	N/A	the gravity of the violations;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(11)	N/A	the number of violations and the length of time over which they occurred;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(12)	N/A	the extent, if any, to which the senior governing body participated therein;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(13)	N/A	any penalty or sanction imposed by any other regulatory agency;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(14)	N/A	the financial resources, net worth and annual business volume of the covered entity and its affiliates;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(15)	N/A	the extent to which the relevant policies and procedures of the company are consistent with nationally recognized cybersecurity frameworks, such as NIST; and	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.20(c)(16)	N/A	such other matters as justice and the public interest require.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.21	Effective Date	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.21(a)	N/A	This Part will be effective March 1, 2017. Covered entities will be required to annually prepare and submit to the superintendent a certification of compliance with New York State Department of Financial Services Cybersecurity Regulations under section 500.17(b) of this Part commencing February 15, 2018.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.21(b)	N/A	The second amendment to this Part shall become effective November 1, 2023.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.22	Transitional Periods	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.22(a)	N/A	Transitional period. Covered entities shall have 180 days from the effective date of this Part to comply with the requirements set forth in this Part, except as otherwise specified.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.22(b)	N/A	The following provisions shall include additional transitional periods. Covered entities shall have:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.22(b)(1)	N/A	one year from the effective date of this Part to comply with the requirements of sections 500.4(b), 500.5, 500.9, 500.12 and 500.14(b) of this Part;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.22(b)(2)	N/A	eighteen months from the effective date of this Part to comply with the requirements of sections 500.6, 500.8, 500.13, 500.14(a) and 500.15 of this Part;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.22(b)(3)	N/A	two years from the effective date of this Part to comply with the requirements of section 500.11 of this Part.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.22(c)	N/A	Covered entities shall have 180 days from the effective date of the second amendment to this Part to comply with the new requirements set forth in the second amendment to this Part, except as otherwise specified in subdivisions (d) and (e) below.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.22(d)	N/A	The following provisions shall include different transitional periods. Covered entities shall have:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.22(d)(1)	N/A	30 days from the effective date of the second amendment to this Part to comply with the new requirements specified in section 500.17 of this Part;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.22(d)(2)	N/A	one year from the effective date of the second amendment to this Part to comply with the new requirements specified in sections 500.4, 500.15, 500.16 and 500.19(a) of this Part;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.22(d)(3)	N/A	18 months from the effective date of the second amendment to this Part to comply with the new requirements specified in sections 500.5(a)(2), 500.7, 500.14(a)(2) and 500.14(b) of this Part; and	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.22(d)(4)	N/A	two years from the effective date of the second amendment to this Part to comply with the new requirements specified in sections 500.12 and 500.13(a) of this Part.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
500.22(e)	N/A	The new requirements specified in sections 500.19(e)-(h), 500.20, 500.21, 500.22 and 500.24 of this Part shall become effective November 1, 2023.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.23	Severability	If any provision of this Part or the application thereof to any person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other persons or circumstances.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.24	Exceptions From Electronic Filing and Submission Requirements	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.24(a)	N/A	A filer required to make an electronic filing or a submission pursuant to this Part may apply to the superintendent for an exemption from the requirement that the filing or submission be electronic by submitting a written request to the superintendent for approval at least 30 days before the filer shall submit to the superintendent the particular filing or submission that is the subject of the request.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.24(b)	N/A	The request for an exemption shall:	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.24(b)(1)	N/A	set forth the filer's DFS license number, NAIC number, Nationwide Multistate Licensing System number or institution number;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.24(b)(2)	N/A	identify the specific filing or submission for which the filer is applying for the exemption;	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.24(b)(3)	N/A	specify whether the filer is making the request for an exemption based upon undue hardship, impracticability or good cause, and set forth a detailed explanation as to the reason that the superintendent should approve the request; and	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.24(b)(4)	N/A	specify whether the request for an exemption extends to future filings or submissions, in addition to the specific filing or submission identified in paragraph (2) of this subdivision.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.24(c)	N/A	The filer requesting an exemption shall submit, upon the superintendent's request, any additional information necessary for the superintendent to evaluate the filer's request for an exemption.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.24(d)	N/A	The filer shall be exempt from the electronic filing or submission requirement upon the superintendent's written determination so exempting the filer, where the determination specifies the basis upon which the superintendent is granting the request and to which filings or submissions the exemption applies.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.24(e)	N/A	If the superintendent approves a filer's request for an exemption from the electronic filing or submission requirement, then the filer shall make a filing or submission in a form and manner acceptable to the superintendent.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.