

# Set Theory Relationship Mapping (STRM)

Reference Document : Secure Controls Framework (SCF) version 2024.1

Focal Document: NY DFS 23 NYCRR500 (December 2023)

STRM URL: <https://content.securecontrolsframework.com/strm/scf-2024-1-ny-dfs-23-nycrr500.pdf>

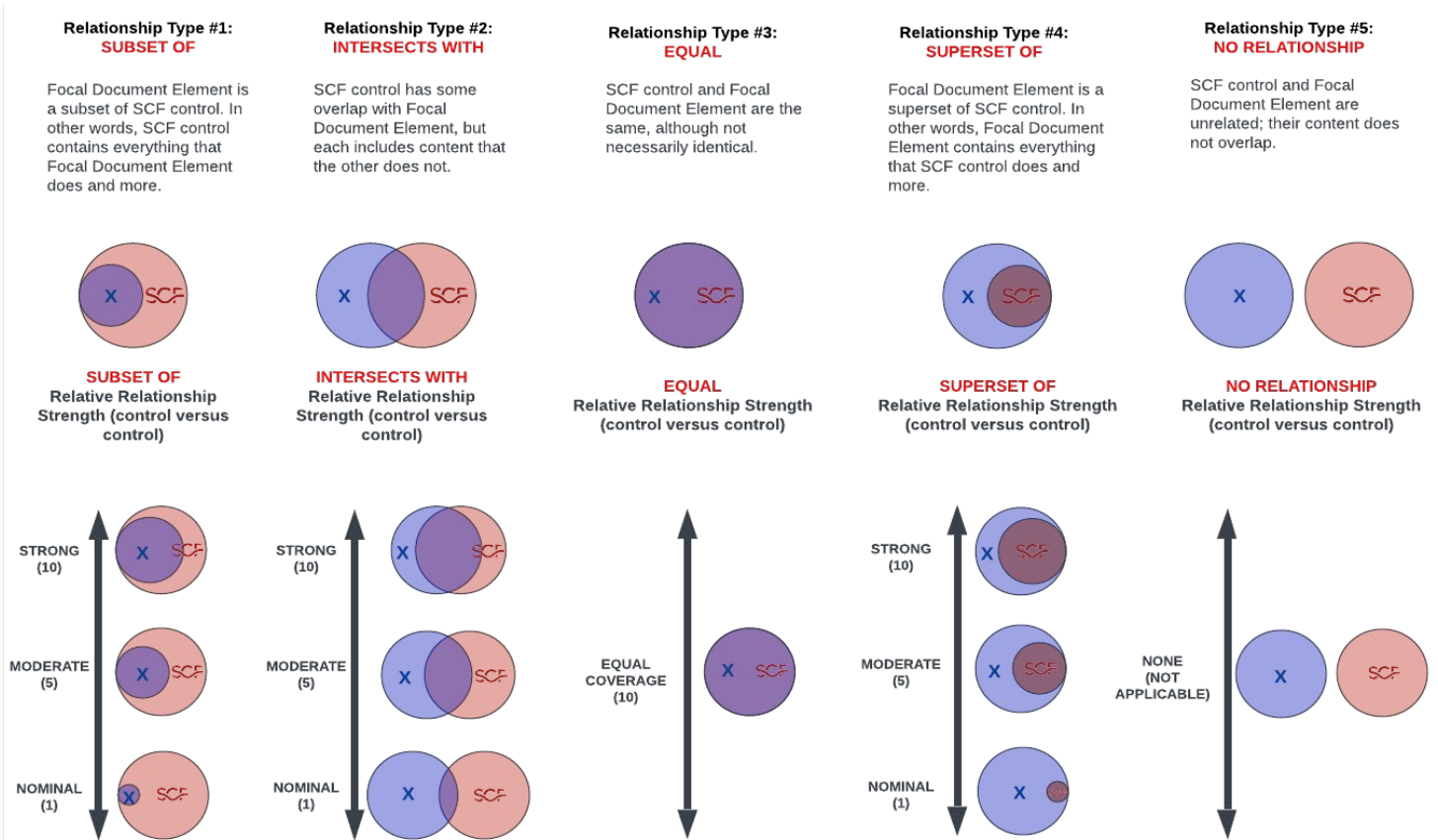
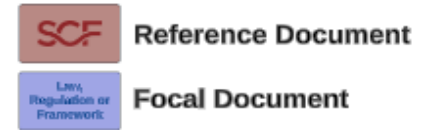
Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

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:

- 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.
- Semantic:** How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
- 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) relationship types to describe the logical similarity between two distinct concepts:

- Subset Of
- Intersects With
- Equal
- Superset Of
- 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)
500.0	Introduction	The New York State Department of Financial Services ("DFS") has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cybersecurity threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success. Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers. It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark. Adoption of the program outlined in these regulations is a priority for New York State.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
500.1	Definitions	(see definitions section for details)	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	Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of 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	
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	
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	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	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	
500.2(b)(3)	N/A	detect Cybersecurity Events;	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)(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	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
500.2(b)(5)	N/A	recover from Cybersecurity Events and restore normal operations and services; and	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)(6)	N/A	fulfill applicable regulatory reporting obligations.	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(c)	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	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(d)	N/A	All documentation and information relevant to the Covered Entity's cybersecurity program 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	
500.3	Cybersecurity Policy	Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address 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.	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)
500.3(a)	N/A	information security;	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	
500.3(b)	N/A	data governance and classification;	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	
500.3(c)	N/A	asset inventory and device management;	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	
500.3(d)	N/A	access controls and identity management;	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	
500.3(e)	N/A	business continuity and disaster recovery planning and resources;	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	
500.3(f)	N/A	systems operations and availability concerns;	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	
500.3(g)	N/A	systems and network security;	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	
500.3(h)	N/A	systems and network monitoring;	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	
500.3(i)	N/A	systems and application development and quality assurance;	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	
500.3(j)	N/A	physical security and environmental controls;	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	
500.3(k)	N/A	customer data privacy;	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	
500.3(l)	N/A	vendor and Third Party Service Provider management;	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	
500.3(m)	N/A	risk assessment; and	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	
500.3(n)	N/A	incident response.	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	
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 qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, "Chief Information Security Officer" or "CISO"). The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider. To the extent this requirement is met using 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 (RASC) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
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 (RASC) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) 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 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 (RASC) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) 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 Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. The CISO shall report on the Covered Entity's cybersecurity program and material cybersecurity risks. The CISO shall consider 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	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	
		the confidentiality of Nonpublic Information and the integrity and security of the	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	

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(b)(1)	N/A	the confidentiality or nonpublic information and the integrity and security of the Covered Entity's Information Systems;	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	
500.4(b)(4)	N/A	overall effectiveness of the Covered Entity's cybersecurity program; 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	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.	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	
500.5	Penetration Testing and Vulnerability Assessments	The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:	Functional	intersects with	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made applications and services.	5	
			Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by recurring vulnerability scanning of systems and web applications.	5	
500.5(a)	N/A	annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and	Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	
			Functional	intersects with	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made applications and services.	5	
500.5(b)	N/A	bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.	Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by recurring vulnerability scanning of systems and web applications.	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	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)(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	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	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
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	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	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	

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	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	As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.	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	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	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	
500.8	Application Security	This is merely a section title without content.	Functional	no relationship	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 periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity.	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	
			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	
500.9	Risk Assessment	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	No requirements to map to.	
500.9(a)	N/A	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 updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. The Covered Entity's Risk 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	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	
			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	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 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 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)(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	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 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 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	

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(b)(3)	N/A	requirements describing how identified risks will be mitigated or accepted based on the RiskAssessment and how the cybersecurity program will address the risks.	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 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-Based Security Categorization	RSK-02	Mechanisms exist to categorize systems and data in accordance with applicable local, state and Federal laws that: <ul style="list-style-type: none"> <li>• Document the security categorization results (including supporting rationale) in the security plan for systems; and</li> <li>• Ensure the security categorization decision is reviewed and approved by the asset owner.</li> </ul>	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 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 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	