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

Focal Document: New York SHIELD Act (SB S5575B) (2019)
Focal Document URL: https://legislation.nysenate.gov/pdf/bills/2019/s5575b
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-ny-shield-act-2019.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1	N/A	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2	N/A	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	Subdivisions 1, 2, 3, 5, 6, 7 and 8 of section 899aa of the general business law, subdivisions 1, 2, 3, 5, 6 and 7 as added by chap ter 442 of the laws of 2005, paragraph (c) of subdivision 1, paragraph (a) of subdivision 6 and subdivision 8 as amended by chapter 491 of the laws of 2005 and paragraph (a) of subdivision 8 as amended by section 6 of part N of chapter 55 of the laws of 2013, are amended, subdivision 9 is renumbered subdivision 10 and a new subdivision 9 is added to read as follows	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.1	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.2	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	Any person or business which [conducts business in New York state, and which] owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the [reasonable] integrity of the syste	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
3.2(a)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials as found in subparagraph (ii) of paragraph (b) of subdivision one of this section. Such a determination must be documented in writing and maintained for at least five years. If the incident affects over five hundred residents of New York, the person or business shall provide the written determination to the state attorney general within ten days after the determination.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
3.2(b)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the department of state and the division of state police pursuant to paragraph (a) of subdivision eight of this section and to consumer reporting agencies pursuant to paragraph (b) of subdivision eight of this section:	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
3.2(b)(i)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	regulations promulgated pursuant to Title V of the federal Gramm LeachBliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.2(b)(ii)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.2(b)(iii)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	part five hundred of title twentythree of the official compila tion of codes, rules and regulations of the state of New York, as amended from time to time; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.2(b)(iv)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	any other data security rules and regulations of, and the stat utes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regu lations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.3	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	Any person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
3.5	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	The notice required by this section shall be directly provided to the affected persons by one of the following methods:	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
3.5(a)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	written notice;	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
3.5(b)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or busi ness who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
3.5(c)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	telephone notification provided that a log of each such notifica tion is kept by the person or business who notifies affect persons; or	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
3.5(d)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	substitute notice, if a business demonstrates to the state attor ney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
3.5(d)(1)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	email notice when such business has an email address for the subject persons, except if the breached information includes an email address in combination with a password or security question and answer that would permit access to the online account, in which case the person or business shall instead provide clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an internet protocol address or from an online location which the person or business knows the consumer customarily uses to access the online accoun	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
3.5(d)(2)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	conspicuous posting of the notice on such business's web site page, if such business maintains one; and	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
3.5(d)(3)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	notification to major statewide media.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
3.6(a)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	whenever the attorney general shall believe from evidence satisfactory to him or her that there is a violation of this article he or she may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be granted under article sixtythree of the civil practice law and rules. In such action the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including conse quential financial losses. Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to [ten] twenty dollars per instance of failed notification, provided that the latter amount shall not exceed [one] two hundred fifty thousand dollars.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3.6(b)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	the remedies provided by this section shall be in addition to any other lawful remedy available.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.6(c)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	no action may be brought under the provisions of this section unless such action is commenced within [two] three years [immediately] after either the date [of the act complained of or the date of discovery of such act] on which the attorney general became aware of the violation, or the date of notice sent pursuant to paragraph (a) of subdivision eight of this section, whichever occurs first. In no event shall an action be brought after six years from the date of discovery of the breach of private information by the company unless the company took steps to hide the breach.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.7	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information, and a description of the categories of information that were, or are reason ably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.8	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.8(a)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	In the event that any New York residents are to be notified, the person or business shall notify the state attorney general, the department of state and the division of state police as to the timing, content and distribution of the notices and approximate number of affected persons and shall provide a copy of the template of the notice sent to affected persons. Such notice shall be made without delaying notice to affected New York residents.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
3.8(b)	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	In the event that more than five thousand New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
3.9	NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS	Any covered entity required to provide notification of a breach, including breach of information that is not "private information" as defined in paragraph (b) of subdivision one of this section, to the secretary of health and human services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, as amended from time to time, shall provide such notification to the state attorney general within five business days of notifying the secretary.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
4	N/A	The general business law is amended by adding a new section 899bb to read as follows	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
899-bb	Data security protections	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
899-bb.1	Definitions	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
899-bb.2	Reasonable security requirement	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
899-bb.2(a)	Reasonable security requirement	Any person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data.	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	8	
899-bb.2(a)	Reasonable security requirement	Any person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	8	
899-bb.2(b)	Reasonable security requirement	A person or business shall be deemed to be in compliance with paragraph (a) of this subdivision if it either:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
899-bb.2(b)(i)	Reasonable security requirement	is a compliant regulated entity as defined in subdivision one of this section; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
899-bb.2(b)(ii)	Reasonable security requirement	implements a data security program that includes the following:	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
899-bb.2(b)(ii)(A)	Reasonable security requirement	reasonable administrative safeguards such as the following, in which the person or business:	Functional	Subset Of	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
899-bb.2(b)(ii)(A)(1)	Reasonable security requirement	designates one or more employees to coordinate the security program;	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
899-bb.2(b)(ii)(A)(2)	Reasonable security requirement	identifies reasonably foreseeable internal and external risks;	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
899-bb.2(b)(ii)(A)(3)	Reasonable security requirement	assesses the sufficiency of safeguards in place to control the identified risks;	Functional	Subset Of	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	10	
899-bb.2(b)(ii)(A)(4)	Reasonable security requirement	trains and manages employees in the security program practices and procedures;	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
899-bb.2(b)(ii)(A)(5)	Reasonable security requirement	selects service providers capable of maintaining appropriate safe guards, and requires those safeguards by contract; and	Functional	Subset Of	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	10	
899-bb.2(b)(ii)(A)(6)	Reasonable security requirement	adjusts the security program in light of business changes or new circumstances; and	Functional	Subset Of	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	10	
899-bb.2(b)(ii)(B)	Reasonable security requirement	reasonable technical safeguards such as the following, in which the person or business:	Functional	Subset Of	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
899-bb.2(b)(ii)(B)	Reasonable security requirement	reasonable technical safeguards such as the following, in which the person or business:	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
899-bb.2(b)(ii)(B)	Reasonable security requirement	reasonable technical safeguards such as the following, in which the person or business:	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
899-bb.2(b)(ii)(B)	Reasonable security requirement	reasonable technical safeguards such as the following, in which the person or business:	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are:(1) Implemented correctly; and(2) Operating as intended.	8	
899-bb.2(b)(ii)(B)	Reasonable security requirement	reasonable technical safeguards such as the following, in which the person or business:	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	8	
899-bb.2(b)(ii)(B)	Reasonable security requirement	reasonable technical safeguards such as the following, in which the person or business:	Functional	Intersects With	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications, Services and/or Data (TAASD) under their control on an ongoing basis for applicable threats and risks, as well as to ensure security, compliance and resilience controls are operating as intended.	8	
899-bb.2(b)(ii)(B)(1)	Reasonable security requirement	assesses risks in network and software design;	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).	8	
899-bb.2(b)(ii)(B)(1)	Reasonable security requirement	assesses risks in network and software design;	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.	8	
899-bb.2(b)(ii)(B)(2)	Reasonable security requirement	assesses risks in information processing, transmission and stor age;	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
899-bb.2(b)(ii)(B)(3)	Reasonable security requirement	detects, prevents and responds to attacks or system failures; and	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	8	
899-bb.2(b)(ii)(B)(4)	Reasonable security requirement	regularly tests and monitors the effectiveness of key controls, systems and procedures; and	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are:(1) Implemented correctly; and(2) Operating as intended.	8	
899-bb.2(b)(ii)(C)	Reasonable security requirement	reasonable physical safeguards such as the following, in which the person or business:	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
899-bb.2(b)(ii)(C)	Reasonable security requirement	reasonable physical safeguards such as the following, in which the person or business:	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	
899-bb.2(b)(ii)(C)(1)	Reasonable security requirement	assesses risks of information storage and disposal;	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to:(1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and(2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	
899-bb.2(b)(ii)(C)(1)	Reasonable security requirement	assesses risks of information storage and disposal;	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
899-bb.2(b)(ii)(C)(1)	Reasonable security requirement	assesses risks of information storage and disposal;	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5	
899-bb.2(b)(ii)(C)(2)	Reasonable security requirement	detects, prevents and responds to intrusions;	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
899-bb.2(b)(ii)(C)(2)	Reasonable security requirement	detects, prevents and responds to intrusions;	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
899-bb.2(b)(ii)(C)(3)	Reasonable security requirement	protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	8	
899-bb.2(b)(ii)(C)(4)	Reasonable security requirement	disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to:(1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law;(2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and(3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	8	
899-bb.2(c)	Reasonable security requirement	A small business as defined in paragraph (c) of subdivision one of this section complies with subparagraph (ii) of paragraph (b) of subdi vision two of this section if the small business's security program contains reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensi tivity of the personal information the small business collects from or about consumers.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
899-bb.2(d)	Reasonable security requirement	Any person or business that fails to comply with this subdivision shall be deemed to have violated section three hundred fortynine of this chapter, and the attorney general may bring an action in the name and on behalf of the people of the state of New York to enjoin such violations and to obtain civil penalties under section three hundred fiftyd of this chapter	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
899-bb.2(e)	Reasonable security requirement	Nothing in this section shall create a private right of action.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5	Reasonable security requirement	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.2	Reasonable security requirement	Any state entity that owns or licenses computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the [reasonable] integ rity of the data system. The state entity shall consult with the state office of information technology services to determine the scope of the breach and restoration measures. Within ninety days of the notice of the breach, the office of information technology services shall deliver a report on the scope of the breach and recommendations to restore and improve the security of the system to the state entity.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
5.2(a)	Reasonable security requirement	Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the state entity reasonably determines such exposure will not likely result in misuse of such information, or financial or emotional harm to the affected persons. Such a determination must be documented in writing and main tained for at least five years. If the incident affected over five hundred residents of New York, the state entity shall provide the writ ten determination to the state attorney general within ten days after the determination.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
5.2(b)	Reasonable security requirement	If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the department of state and the office of information technology services pursuant to paragraph (a) of subdivision seven of this section and to consumer reporting agencies pursuant to paragraph (b) of subdivision seven of this section:	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
5.2(b)(i)	Reasonable security requirement	regulations promulgated pursuant to Title V of the federal Gramm LeachBliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.2(b)(ii)	Reasonable security requirement	regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.2(b)(iii)	Reasonable security requirement	part five hundred of title twentythree of the official compila tion of codes, rules and regulations of the state of New York, as amended from time to time; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.2(b)(iv)	Reasonable security requirement	any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regu lations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.3	Reasonable security requirement	Any state entity that maintains computerized data that includes private information which such agency does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
5.6	Reasonable security requirement	Regardless of the method by which notice is provided, such notice 42 shall include contact information for the state entity making the 43 notification, the telephone numbers and websites of the relevant state 44 and federal agencies that provide information regarding security breach response and identity theft prevention and protection information and a description of the categories of information that were, or are reason ably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
5.7(a)	Reasonable security requirement	In the event that any New York residents are to be notified, the state entity shall notify the state attorney general, the department of state and the state office of information technology services as to the timing, content and distribution of the notices and approximate number of affected persons and provide a copy of the template of the notice sent to affected persons. Such notice shall be made without delaying notice to affected New York residents.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
5.7(b)	Reasonable security requirement	In the event that more than five thousand New York residents are to be notified at one time, the state entity shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
5.8	Reasonable security requirement	The state office of information technology services shall develop, update and provide regular training to all state entities relating to best practices for the prevention of a breach of the security of the system.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
5.9	Reasonable security requirement	Any covered entity required to provide notification of a breach, including breach of information that is not "private information" as defined in paragraph (a) of subdivision one of this section, to the secretary of health and human services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, as amended from time to time, shall provide such notification to the state attorney general within five business days of notifying the secretary.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
5.10	Reasonable security requirement	Any entity listed in subparagraph two of paragraph (c) of subdi vision one of this section shall adopt a notification policy no more than one hundred twenty days after the effective date of this section. Such entity may develop a notification policy which is consistent with this section or alternatively shall adopt a local law which is consist ent with this section	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
6	N/A	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control