NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2025.3
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: NAIC Insurance Data Security Model Law (#668)
Focal Document URL: https://content.naic.org/sites/default/files/model-law-668.pdf
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-general-naic-insurance-data-security-model-law-668.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 (optional)	Notes (optional)
1	Title	This Act shall be known and may be cited as the "Insurance Data Security Law."	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
2	Purpose and Intent	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
2.A	N/A	The purpose and intent of this Act is to establish standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to Licensees, as defined in Section 3.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
2.B	N/A	This Act may not be construed to create or imply a private cause of action for violation of its provisions nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
3	Definitions	See source for specific definitions.	Functional	Subset of	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	10	
4	Information Security Program	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
4.A	Implementation of an Information Security Program	Commensurate with the size and complexity of the Licensee, the nature and scope of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody or control, each Licensee shall develop, implement, and maintain a comprehensive written Information Security Program based on the Licensee's Risk Assessment and that contains administrative, technical, and physical safeguards for the protection of Nonpublic Information and the Licensee's Information System.	Functional	Subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
4.B	Objectives of Information Security Program	A Licensee's Information Security Program shall be designed to:	Functional	Subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
4.B(1)	N/A	Protect the security and confidentiality of Nonpublic Information and the security of the Information System;	Functional	Subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
4.B(2)	N/A	Protect against any threats or hazards to the security or integrity of Nonpublic Information and the Information System;	Functional	Subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
4.B(3)	N/A	Protect against unauthorized access to or use of Nonpublic Information, and minimize the likelihood of harm to any Consumer; and	Functional	Subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
4.B(4)	N/A	Define and periodically reevaluate a schedule for retention of Nonpublic Information and a mechanism for its destruction when no longer needed.	Functional	Subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
4.B(4)	N/A	Define and periodically reevaluate a schedule for retention of Nonpublic Information and a mechanism for its destruction when no longer needed.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	8	
4.C	Risk Assessment	The Licensee shall:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
4.C(1)	N/A	Designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the Licensee who is responsible for the Information Security Program;	Functional	Subset of	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 and data protection program.	10	
4.C(2)	N/A	Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of Nonpublic Information, including the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third-Party Service Providers;	Functional	Subset of	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.	10	
4.C(2)	N/A	Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of Nonpublic Information, including the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third-Party Service Providers;	Functional	Subset of	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.	10	
4.C(3)	N/A	Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Nonpublic Information;	Functional	Subset of	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.	10	
4.C(4)	N/A	Assess the sufficiency of policies, procedures, Information Systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the Licensee's operations, including:	Functional	Subset of	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	10	
4.C(4)	N/A	Assess the sufficiency of policies, procedures, Information Systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the Licensee's operations, including:	Functional	Subset of	Cybersecurity and Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements.	10	
4.C(4)	N/A	Assess the sufficiency of policies, procedures, Information Systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the Licensee's operations, including:	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's cybersecurity and data protection policies and standards.	8	
4.C(4)(a)	N/A	Employee training and management;	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	8	
4.C(4)(a)	N/A	Employee training and management;	Functional	Intersects With	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	8	
4.C(4)(b)	N/A	Information Systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal; and	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	8	
4.C(4)(b)	N/A	Information Systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal; and	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
4.C(4)(b)	N/A	Information Systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal; and	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	
4.C(4)(c)	N/A	Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	8	
4.C(4)(c)	N/A	Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and	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 and data protection-related incidents.	8	
4.C(5)	N/A	Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.	Functional	Intersects With	Cybersecurity and Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements.	8	
4.C(5)	N/A	Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's cybersecurity and data protection policies and standards.	8	
4.C(5)	N/A	Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
4.C(5)	N/A	Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.	Functional	Subset of	Threat Intelligence 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.	10	
4.C(5)	N/A	Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.	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.	8	

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)
4.C(5)	N/A	Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.	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.	8	
4.D	Risk Management	Based on its Risk Assessment, the Licensee shall:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
4.D(1)	N/A	Design its Information Security Program to mitigate the identified risks, commensurate with the size and complexity of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody, or control.	Functional	Subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
4.D(1)	N/A	Design its Information Security Program to mitigate the identified risks, commensurate with the size and complexity of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody, or control.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
4.D(2)	N/A	Determine which security measures listed below are appropriate and implement such security measures.	Functional	Subset of	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	10	
4.D(2)(a)	N/A	Place access controls on Information Systems, including controls to authenticate and permit access only to Authorized Individuals to protect against the unauthorized acquisition of Nonpublic Information;	Functional	Subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
4.D(2)(b)	N/A	Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	8	
4.D(2)(b)	N/A	Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
4.D(2)(b)	N/A	Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	
4.D(2)(b)	N/A	Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;	Functional	Intersects With	Cybersecurity & Data Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection-related resource planning controls that define a viable plan for achieving cybersecurity and data protection objectives.	8	
4.D(2)(b)	N/A	Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;	Functional	Intersects With	Cybersecurity & Data Protection Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity and data protection programs and document all exceptions to this requirement.	8	
4.D(2)(b)	N/A	Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
4.D(2)(c)	N/A	Restrict access at physical locations containing Nonpublic Information, only to Authorized Individuals;	Functional	Subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
4.D(2)(c)	N/A	Restrict access at physical locations containing Nonpublic Information, only to Authorized Individuals;	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	8	
4.D(2)(d)	N/A	Protect by encryption or other appropriate means, all Nonpublic Information while being transmitted over an external network and all Nonpublic Information stored on a laptop computer or other portable computing or storage device or media;	Functional	Subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
4.D(2)(d)	N/A	Protect by encryption or other appropriate means, all Nonpublic Information while being transmitted over an external network and all Nonpublic Information stored on a laptop computer or other portable computing or storage device or media;	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
4.D(2)(d)	N/A	Protect by encryption or other appropriate means, all Nonpublic Information while being transmitted over an external network and all Nonpublic Information stored on a laptop computer or other portable computing or storage device or media;	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
4.D(2)(e)	N/A	Adopt secure development practices for in-house developed applications utilized by the Licensee and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Licensee;	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	
4.D(2)(e)	N/A	Adopt secure development practices for in-house developed applications utilized by the Licensee and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Licensee;	Functional	Intersects With	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	8	
4.D(2)(f)	N/A	Modify the Information System in accordance with the Licensee's Information Security Program;	Functional	Subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
4.D(2)(g)	N/A	Utilize effective controls, which may include Multi-Factor Authentication procedures for any individual accessing Nonpublic Information;	Functional	Intersects With	Business As Usual (BAU) Secure Practices	GOV-14	Mechanisms exist to incorporate cybersecurity and data protection principles into Business As Usual (BAU) practices through executive leadership involvement.	5	
4.D(2)(g)	N/A	Utilize effective controls, which may include Multi-Factor Authentication procedures for any individual accessing Nonpublic Information;	Functional	Intersects With	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each system, application and/or service under their control.	8	
4.D(2)(g)	N/A	Utilize effective controls, which may include Multi-Factor Authentication procedures for any individual accessing Nonpublic Information;	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5	
4.D(2)(h)	N/A	Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, Information Systems;	Functional	Subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
4.D(2)(i)	N/A	Include audit trails within the Information Security Program designed to detect and respond to Cybersecurity Events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Licensee;	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	8	
4.D(2)(i)	N/A	Include audit trails within the Information Security Program designed to detect and respond to Cybersecurity Events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Licensee;	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	8	
4.D(2)(j)	N/A	Implement measures to protect against destruction, loss, or damage of Nonpublic Information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
4.D(2)(j)	N/A	Implement measures to protect against destruction, loss, or damage of Nonpublic Information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	
4.D(2)(j)	N/A	Implement measures to protect against destruction, loss, or damage of Nonpublic Information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and	Functional	Intersects With	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	8	
4.D(2)(j)	N/A	Implement measures to protect against destruction, loss, or damage of Nonpublic Information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and	Functional	Intersects With	Water Damage Protection	PES-07.5	Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key personnel.	8	
4.D(2)(j)	N/A	Implement measures to protect against destruction, loss, or damage of Nonpublic Information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and	Functional	Intersects With	Fire Protection	PES-08	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	8	
4.D(2)(k)	N/A	Develop, implement, and maintain procedures for the secure disposal of Nonpublic Information in any format.	Functional	Subset of	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	10	
4.D(3)	N/A	Include cybersecurity risks in the Licensee's enterprise risk management process.	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)
4.D(4)	N/A	Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and	Functional	Subset of	Threat Intelligence 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.	10	
4.D(4)	N/A	Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and	Functional	Subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
4.D(5)	N/A	Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the Licensee in the Risk Assessment.	Functional	Intersects With	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	8	
4.D(5)	N/A	Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the Licensee in the Risk Assessment.	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	
4.E	Oversight by Board of Directors	If the Licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
4.E(1)	N/A	Require the Licensee's executive management or its delegates to develop, implement, and maintain the Licensee's Information Security 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	
4.E(2)	N/A	Require the Licensee's executive management or its delegates to report in writing at least annually, the following information:	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	
4.E(2)(a)	N/A	The overall status of the Information Security Program and the Licensee's compliance with this Act; 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	
4.E(2)(b)	N/A	Material matters related to the Information Security Program, addressing issues such as risk assessment, risk management and control decisions, Third-Party Service Provider arrangements, results of testing, Cybersecurity Events or violations and management's responses thereto, and recommendations for changes in the Information Security 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	
4.E(2)(b)	N/A	Material matters related to the Information Security Program, addressing issues such as risk assessment, risk management and control decisions, Third-Party Service Provider arrangements, results of testing, Cybersecurity Events or violations and management's responses thereto, and recommendations for changes in the Information Security Program.	Functional	Intersects With	Materiality Determination	GOV-16	Mechanisms exist to define materiality threshold criteria capable of designating an incident as material.	8	
4.E(2)(b)	N/A	Material matters related to the Information Security Program, addressing issues such as risk assessment, risk management and control decisions, Third-Party Service Provider arrangements, results of testing, Cybersecurity Events or violations and management's responses thereto, and recommendations for changes in the Information Security Program.	Functional	Intersects With	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5	
4.E(2)(b)	N/A	Material matters related to the Information Security Program, addressing issues such as risk assessment, risk management and control decisions, Third-Party Service Provider arrangements, results of testing, Cybersecurity Events or violations and management's responses thereto, and recommendations for changes in the Information Security Program.	Functional	Intersects With	Material Threats	GOV-16.2	Mechanisms exist to define criteria necessary to designate a threat as a material threat.	5	
4.E(2)(b)	N/A	Material matters related to the Information Security Program, addressing issues such as risk assessment, risk management and control decisions, Third-Party Service Provider arrangements, results of testing, Cybersecurity Events or violations and management's responses thereto, and recommendations for changes in the Information Security Program.	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.	8	
4.E(3)	N/A	If executive management delegates any of its responsibilities under Section 4 of this Act, it shall oversee the development, implementation and maintenance of the Licensee's Information Security Program prepared by the delegate(s) and shall receive a report from the delegate(s) complying with the requirements of the report to the Board of Directors above.	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	
4.F	Oversight of Third-Party Service Provider Arrangements	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
4.F(1)	N/A	A Licensee shall exercise due diligence in selecting its 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	
4.F(2)	N/A	A Licensee shall require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures to protect and secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider.	Functional	Subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
4.G	Program Adjustments	The Licensee shall monitor, evaluate and adjust, as appropriate, the Information Security Program consistent with any relevant changes in technology, the sensitivity of its Nonpublic Information, internal or external threats to information, and the Licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to Information Systems.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	8	
4.H	Incident Response Plan	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
4.H(1)	N/A	As part of its Information Security Program, each Licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event that compromises the confidentiality, integrity, or availability of Nonpublic Information in its possession, the Licensee's Information Systems, or the continuing functionality of any aspect of the Licensee's business or operations.	Functional	Equal	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	
4.H(2)	N/A	Such incident response plan shall address the following areas:	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	
4.H(2)(a)	N/A	The internal process for responding to a Cybersecurity Event;	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	
4.H(2)(b)	N/A	The goals of the incident response plan;	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	
4.H(2)(c)	N/A	The definition of clear roles, responsibilities and levels of decision-making authority;	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	
4.H(2)(d)	N/A	External and internal communications and information sharing;	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	
4.H(2)(e)	N/A	Identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;	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	
4.H(2)(f)	N/A	Documentation and reporting regarding Cybersecurity Events and related incident response activities; and	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	
4.H(2)(g)	N/A	The evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.	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	
4.I	Annual Certification to Commissioner of Domiciliary State	Annually, each insurer domiciled in this State shall submit to the Commissioner, a written statement by February 15, certifying that the insurer is in compliance with the requirements set forth in Section 4 of this Act. Each insurer shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years. To the extent an insurer has identified areas, systems, or processes that require material improvement, updating or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the Commissioner.	Functional	Intersects With	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	8	
5	Investigation of a Cybersecurity Event	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	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)
5.A	N/A	If the Licensee learns that a Cybersecurity Event has or may have occurred the Licensee or an outside vendor and/or service provider designated to act on behalf of the Licensee, shall conduct a prompt investigation.	Functional	Subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
5.B	N/A	During the investigation, the Licensee, or an outside vendor and/or service provider designated to act on behalf of the Licensee, shall, at a minimum determine as much of the following information as possible:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
5.B(1)	N/A	Determine whether a Cybersecurity Event has occurred;	Functional	Subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
5.B(2)	N/A	Assess the nature and scope of the Cybersecurity Event;	Functional	Subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
5.B(3)	N/A	Identify any Nonpublic Information that may have been involved in the Cybersecurity Event; and	Functional	Subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
5.B(4)	N/A	Perform or oversee reasonable measures to restore the security of the Information Systems compromised in the Cybersecurity Event in order to prevent further unauthorized acquisition, release or use of Nonpublic Information in the Licensee's possession, custody or control.	Functional	Subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
5.C	N/A	If the Licensee learns that a Cybersecurity Event has or may have occurred in a system maintained by a Third-Party Service Provider, the Licensee will complete the steps listed in Section 5B above or confirm and document that the Third-Party Service Provider has completed those steps.	Functional	Subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
5.D	N/A	The Licensee shall maintain records concerning all Cybersecurity Events for a period of at least five years from the date of the Cybersecurity Event and shall produce those records upon demand of the Commissioner	Functional	Subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
6	Notification of a Cybersecurity Event	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
6.A	Notification to the Commissioner	Each Licensee shall notify the Commissioner as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred when either of the following criteria has been met:	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.A(1)	N/A	This State is the Licensee's state of domicile, in the case of an insurer, or this State is the Licensee's home state, in the case of a producer, as those terms are defined in [insert reference to Producer Licensing Model Act]; or	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.A(2)	N/A	The Licensee reasonably believes that the Nonpublic Information involved is of 250 or more Consumers residing in this State and that is either of the following:	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.A(2)(a)	N/A	A Cybersecurity Event impacting the Licensee of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body pursuant to any state or federal law; or	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.A(2)(b)	N/A	A Cybersecurity Event that has a reasonable likelihood of materially harming:	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.A(2)(b)(i)	N/A	Any Consumer residing in this State; or	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.A(2)(b)(ii)	N/A	Any material part of the normal operation(s) of the Licensee.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.B	N/A	The Licensee shall provide as much of the following information as possible. The Licensee shall provide the information in electronic form as directed by the Commissioner. The Licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Commissioner concerning the Cybersecurity Event.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.B(1)	N/A	Date of the Cybersecurity Event;	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.B(2)	N/A	Description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of Third-Party Service Providers, if any;	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.B(3)	N/A	How the Cybersecurity Event was discovered;	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.B(4)	N/A	Whether any lost, stolen, or breached information has been recovered and if so, how this was done;	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.B(5)	N/A	The identity of the source of the Cybersecurity Event;	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.B(6)	N/A	Whether Licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.B(7)	N/A	Description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information or types of information allowing identification of the Consumer;	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.B(8)	N/A	The period during which the Information System was compromised by the Cybersecurity Event;	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.B(9)	N/A	The number of total Consumers in this State affected by the Cybersecurity Event. The Licensee shall provide the best estimate in the initial report to the Commissioner and update this estimate with each subsequent report to the Commissioner pursuant to this section;	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.B(10)	N/A	The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.B(11)	N/A	Description of efforts being undertaken to remediate the situation which permitted the Cybersecurity Event to occur;	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.B(12)	N/A	A copy of the Licensee's privacy policy and a statement outlining the steps the Licensee will take to investigate and notify Consumers affected by the Cybersecurity Event; and	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.B(13)	N/A	Name of a contact person who is both familiar with the Cybersecurity Event and authorized to act for the Licensee.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	

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)
6.C	N/A	Notification to Consumers. Licensee shall comply with [insert state's data breach notification law], as applicable, and provide a copy of the notice sent to Consumers under that statute to the Commissioner, when a Licensee is required to notify the Commissioner under Section 6A.	Functional	Subset of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
6.D	Notice Regarding Cybersecurity Events of Third-Party Service Providers	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
6.D(1)	N/A	In the case of a Cybersecurity Event in a system maintained by a Third-Party Service Provider, of which the Licensee has become aware, the Licensee shall treat such event as it would under Section 6A	Functional	Subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
6.D(2)	N/A	The computation of Licensee's deadlines shall begin on the day after the Third-Party Service Provider notifies the Licensee of the Cybersecurity Event or the Licensee otherwise has actual knowledge of the Cybersecurity Event, whichever is sooner.	Functional	Subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
6.D(2)	N/A	The computation of Licensee's deadlines shall begin on the day after the Third-Party Service Provider notifies the Licensee of the Cybersecurity Event or the Licensee otherwise has actual knowledge of the Cybersecurity Event, whichever is sooner.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.D(3)	N/A	Nothing in this Act shall prevent or abrogate an agreement between a Licensee and another Licensee, a Third-Party Service Provider or any other party to fulfill any of the investigation requirements imposed under Section 5 or notice requirements imposed under Section 6.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
6.E	Notice Regarding Cybersecurity Events of Reinsurers to Insurers	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
6.E(1)	N/A	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
6.E(1)(a)	N/A	In the case of a Cybersecurity Event involving Nonpublic Information that is used by the Licensee that is acting as an assuming insurer or in the possession, custody or control of a Licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected Consumers, the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of making the determination that a Cybersecurity Event has occurred.	Functional	Intersects With	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.	8	
6.E(1)(b)	N/A	The ceding insurers that have a direct contractual relationship with affected Consumers shall fulfill the consumer notification requirements imposed under [insert the state's breach notification law] and any other notification requirements relating to a Cybersecurity Event imposed under Section 6.	Functional	Intersects With	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.	8	
6.E(2)	N/A	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
6.E(2)(a)	N/A	In the case of a Cybersecurity Event involving Nonpublic Information that is in the possession, custody or control of a Third-Party Service Provider of a Licensee that is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of receiving notice from its Third-Party Service Provider that a Cybersecurity Event has occurred.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.E(2)(b)	N/A	The ceding insurers that have a direct contractual relationship with affected Consumers shall fulfill the consumer notification requirements imposed under [insert the state's breach notification law] and any other notification requirements relating to a Cybersecurity Event imposed under Section 6.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
6.F	Notice Regarding Cybersecurity Events of Insurers to Producers of Record	In the case of a Cybersecurity Event involving Nonpublic Information that is in the possession, custody or control of a Licensee that is an insurer or its Third-Party Service Provider and for which a Consumer accessed the insurer's services through an independent insurance producer, the insurer shall notify the producers of record of all affected Consumers as soon as practicable as directed by the Commissioner. The insurer is excused from this obligation for those instances in which it does not have the current producer of record information for any individual Consumer.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
7	Power of Commissioner	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
7.A	N/A	The Commissioner shall have power to examine and investigate into the affairs of any Licensee to determine whether the Licensee has been or is engaged in any conduct in violation of this Act. This power is in addition to the powers which the Commissioner has under [insert applicable statutes governing the investigation or examination of insurers]. Any such investigation or examination shall be conducted pursuant to [insert applicable statutes governing the investigation or examination of insurers].	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
7.B	N/A	Whenever the Commissioner has reason to believe that a Licensee has been or is engaged in conduct in this State which violates this Act, the Commissioner may take action that is necessary or appropriate to enforce the provisions of this Act.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
8	Confidentiality	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
8.A	N/A	Any documents, materials or other information in the control or possession of the Department that are furnished by a Licensee or an employee or agent thereof acting on behalf of Licensee pursuant to Section 4I, Section 6B(2), (3), (4), (5), (8), (10), and (11), or that are obtained by the Commissioner in an investigation or examination pursuant to Section 7 of this Act shall be confidential by law and privileged, shall not be subject to [insert reference to state open records, freedom of information, sunshine or other appropriate law], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the Commissioner is authorized to use the documents, materials or other information in the furtherance of any regulatory or legal action brought as a part of the Commissioner's duties.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
8.B	N/A	Neither the Commissioner nor any person who received documents, materials or other information while acting under the authority of the Commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to Section 8A.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
8.C	N/A	In order to assist in the performance of the Commissioner's duties under this Act, the Commissioner:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
8.C(1)	N/A	May share documents, materials or other information, including the confidential and privileged documents, materials or information subject to Section 8A, with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material or other information;	Functional	No relationship	N/A	N/A	No applicable SCF control	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)
8.C(2)	N/A	May receive documents, materials or information, including otherwise confidential and privileged documents, materials or information, from the National Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material or information;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
8.C(3)	N/A	May share documents, materials or other information subject to Section 8A, with a thirdparty service provider or vendor provided the third-party service provider or vendor agrees in writing to maintain the confidentiality and privileged status of the document, material or other information; and	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
8.C(4)	N/A	May enter into agreements governing sharing and use of information consistent with this subsection.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
8.D	N/A	No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the Commissioner under this section or as a result of sharing as authorized in Section 8C.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
8.E	N/A	Nothing in this Act shall prohibit the Commissioner from releasing final, adjudicated actions that are open to public inspection pursuant to [insert appropriate reference to state law] to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
9	Exceptions	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
9.A	N/A	The following exceptions shall apply to this Act:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
9.A(1)	N/A	A Licensee with fewer than ten employees, including any independent contractors, is exempt from Section 4 of this Act;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
9.A(2)	N/A	A Licensee subject to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996 (Health Insurance Portability and Accountability Act) that has established and maintains an Information Security Program pursuant to such statutes, rules, regulations, procedures or guidelines established thereunder, will be considered to meet the requirements of Section 4, provided that Licensee is compliant with, and submits a written statement certifying its compliance with, the same;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
9.A(3)	N/A	An employee, agent, representative or designee of a Licensee, who is also a Licensee, is exempt from Section 4 and need not develop its own Information Security Program to the extent that the employee, agent, representative or designee is covered by the Information Security Program of the other Licensee.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
9.B	N/A	In the event that a Licensee ceases to qualify for an exception, such Licensee shall have 180 days to comply with this Act.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
10	Penalties	In the case of a violation of this Act, a Licensee may be penalized in accordance with [insert general penalty statute].	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
11	Rules and Regulations	The Commissioner may, in accordance with [the state statute setting forth the ability of the Department to adopt regulations] issue such regulations as shall be necessary to carry out the provisions of this Act.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
12	Severability	If any provisions of this Act or the application thereof to any person or circumstance is for any reason held to be invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected thereby.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
13	Effective Date	This Act shall take effect on [insert a date]. Licensees shall have one year from the effective date of this Act to implement Section 4 of this Act and two years from the effective date of this Act to implement Section 4F of this Act.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	