NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2025.2
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document III.
Focal Document IVII.
Focal Docu

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 (optional)
17 CFR 229.105(a)	N/A	Where appropriate, provide under the caption "Risk Factors" a discussion of the material factors that make an investment in the registrant or offering speculative or risky. This discussion must be organized logically with relevant headings and each risk factor should be set forth under a subcapplion that safequately describes the risk. The presentation of risks that could apply generically to any registrant or early offering is discouraged, but to the sent engeneric risk storcs are presented, disclose them at the end of the risk factor section under the caption "General Risk Factors."	Functional	intersects with	Materiality Determination	GOV-16	Mechanisms exist to define materially threshold criteria capable of designating an incident as material.	5	
17 CFR 229.105(a)	N/A	Where appropriate, provide under the caption "Risk Factors" a discussion of the material factors that make an investment in the registrant or offering speculative or risky. This discussion must be organized logically with relevant headings and each risk factor should be set forth under a subcappion that adequately describes the risk. The presentation of risks that could apply generically to any registrant or any offering is discouraged, but to the extent generic risk factors are presented, disclose them at the end of the risk factor section under the caption "General Risk Factors."	Functional	intersects with	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5	
17 CFR 229.105(a)	N/A	Where appropriate, provide under the caption "fails Factors" a discussion of the material factors that make an investment in the registrant or offering speculative or risky. This discussion must be organized logically with relevant headings and each risk factor should be set forth under a subcaption that adequately describes the risk. The presentation of risks that could apply generically to any registrant or your offering is discouraged, but to the extent generic risk factors are presented, disclose them at the end of the risk factor section under the caption "General Risk Factors."	Functional	intersects with	Material Threats	GOV-16.2	Mechanisms exist to define criteria necessary to designate a threat as a material threat.	5	
17 CFR 229.105(a)	N/A	Where appropriate, provide under the caption "Risk Factors" a discussion of the material factors that make an investment in the registrant or offering speculative or risky. This discussion must be organized logically with relevant headings and each risk factor should be set forth under subcaption that adequately describes the risk. The presentation of risks that could apply generically to any registrant or any offering is allocuraged, but to the extent generic risk factors are presented, disclose them at the end of the risk factor section under the caption "General Risk Factors."	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
17 CFR 229.105(a)	N/A	Where appropriate, provide under the caption "Risk Factors" a discussion of the material factors that make an investment in the registrant or offering speculative or risky. This discussion must be organized logically with relevant headings and each risk factor elsould be set forth under subcaption that adequately describes the risk. The presentation of risks that could apply generically to any registrant or any offering is allocuraged, but to the extent generic risk factors are presented, disclose them at the end of the risk factor section under the caption "General Risk Factors."	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: (I) Assumptions affecting risk assessments, risk response and risk monitoring: [2] Constraints affecting risk assessments, risk response and risk monitoring: (3) The organizational risk tolerance; and (4) Piorities, benefits and trade-offs considered by the organization for management risk.	5	
17 CFR 229.105(a)	N/A	Where appropriate, provide under the caption "Risk Factors" a discussion of the material factors that make an investment in the registrant or offering speculative or risky. This discussion must be organized logically with relevant headings and each risk factor should be set forth under subcappion that adequately describes the risk. The presentation of risks that could apply generically to any registrant or any offering is discouraged, but to the extent generic risk factors are presented, disclose them at the end of the risk factor section under the caption "General Risk Factors."	Functional	intersects with	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize systems and data in accordance with applicable laws, regulations and contractual obligations that: (1) Document the sacurity categorization results (including supporting rationals) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5	
17 CFR 229.105(a)	N/A	Where appropriate, provide under the caption "Risk Factors" a discussion of the material factors that make an investment in the registrant or offering speculative or risky. This discussion must be organized logically with relevant headings and each risk factor should be set forth under subcoppion that adequately describes the risk. The presentation of risks that could apply generically to any registrant or any offering is discouraged, but to the extent generic risk factors are presented, disclose them at the end of the risk factor section under the caption "General Risk Factors."	Functional	intersects with	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	
17 CFR 229.105(a)	N/A	Where appropriate, provide under the caption "Risk Factors" a discussion of the material factors that make an investment in the registrant or offering speculative or risky. This discussion must be organized logically with relevant headings and each risk factor should be set forth under a subcaption that sideousledy describes the risk. The presentation of risks that could apply generically to any registrant or any offering is discouraged, but to the extent generic risk storcs are presented, disclose them at the end of the risk factor section under the caption "General Risk Factors."	Functional	intersects with	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
17 CFR 229.105(b)	N/A	Concisely explain how each risk affects the registrant or the securities being offered. If the discussion is longer than 15 pages, include in the forepart of the prospectus or annual report, as applicable, a series of concise, butled or numbered statements that is no more than two pages unamarating the principal factors that make an investment in the registrant or offering speculative or risk; if the strateor discussion is included in a registration statement, it must immediately follow the summary section required by \$2.29.503 (files 1950 of Regulation S-R, if you do not include a summary section, the risk factor discussion is included in a registration that even the prospectus or or the princing information section that immediately follows the cover page. Princing information means price and price-related information that you may onlint from the prospectus in an effective registration statement based on Rule 430A (520.430A of this chapter). The registrant must furnish this information in plain English. See 8 200.421(i) of Registation of this inchapter.	Functional	intersects with	Materiality Determination	GOV-16	Mechanisms exist to define materiality threshold criteria capable of designating an incident as material.	5	
17 CFR 229.105(b)	N/A	Conclesely explain how each risk affects the registrant or the securities being offered. If the discussion is longer than 15 pages, include in the forepart of the prospectus or annual report, as applicable, a series of concise, builded or numbered statements that is no more than two pages summarizing the principal factors that make an investment in the registrant or offering speculative or risk; If the risk factor discussion is included in a registration statement, it must immediately follow the summary section required by \$2.29.503 (filem 503 of Regulation S-R, If you do not include a summary section, the risk factor discussion is included in a registration that cover page. If you do not include a summary section, the risk factor action must immediately follows the cover page. Pricing information man price and price-related information that you may only from the prospectus in a reflective registration statement based on Rule 430A (520.430A) of this chapter). The registrant must furnish this information in plain English. See § 20.04.24(i) of Registation of this inchapter.	Functional	intersects with	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5	
17 CFR 229.105(b)	N/A	Concless) explain how each risk affects the egistant or the securities being offeed. If the discussion is longer than 15 pages, include in the forepart of the prospectus or annual report, as applicable, a series of concles, builded or numbered statements that is no more than two pages summarizing the principal factors that make an investment in the registrant or offering speculative or risk; If the first factor discussion is included in a registration statement, it must immediately follow the summary section required by \$2.25.030 (them 503 of Regulation S-14, If you do not include a summary section, the risk factor described in templation of the prospectus or the principal immediately follows the cover page. Princip information means price and prior-related unformation that you may only from the prospectus in an effective registration statement based on Rule 430A (5.20.430A of this chapter). The registrant must furnish this information in plain English. See § 20.04.2(ii) of Registation of of this chapter.	Functional	intersects with	Material Threats	GOV-16.2	Mechanisms exist to define criteria necessary to designate a threat as a material threat.	5	
17 CFR 229.105(b)	N/A	Conclesely explain how each risk affects the negistrant or the securities being offered. If the discussion is longer than 15 pages, include in the repeat of the prospectur or annual report, as applicable, a series of conclese, bulleted or numbered statements that is no more than two pages summarizing the principal factors that make an investment in the registrant or offering specialised or risky. If the six factor discussion is included in a registration statement, it must immediately follow the summary section required by \$2.29.203 (tiem 503 of Regulation 9-14, if you do not include a summary section, the risk factor described in the six of	Functional	subset of	Cybersecurity & Data Privacy Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's opbersecurity and/ordat privacy program to applicable statutory and/or regulatory authorities, as required.	10	
17 CFR 229.105(b)	NA	Conclesely explain how each risk affects the registrant or the excursive being offered. If the discussion is longer than 15 pages, include in the forepart of the prospectus or annual report, as applicable, a series of concise, builded or numbered statements that is no more than two pages summarizing the principal factors that make an investment in the registrant or offering speculative or risky. If the risk factor discussion is included in a registration statement, it must immediately follow the summary section required by \$225,000 (them 500 of Regulation (3). If you do not include a summary section, the risk exciton that immediately follows the cover page. Pricing information means page can be considered in the control of the page of the control of the page of the cover page. Pricing information means page on any price-related information that you may omit from the prospectual is an effective registration statement based on Rula 4004 (8.204.04.05 of this chapter). The registrant must turnish this information in plain English. See § 200.421(d) of Regulation C of this chapter.	Functional	intersects with	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize systems and data in accordance with specificable laws, equilations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security categorization results (including supporting rationale) in the security plant for systems; and 22 Ensure the security categorization decision is reviewed and approved by the asset owner.	5	
17 CFR 229.105(b)	N/A	Concludy explain how each risk affects the registrant or the securities being offered. If the discussion longer than 15 pages, include in the forepart of the prospect or annual report, as applicable, seemed of conclus, buillated or numbered statements that is no more than two pages summarizing the principal factors that make an investment in the registrant or offering speculative or sixty. When risk factor discussion is included in a registration statement, It must immediately follow the summary section expected by \$2.95.00 (tem \$5.00 feeplation 5-V), If you do not includes a summary section, the risk factor section must immediately follow the cover page of the prospectus or the princip information action that immediately follow the cover page affect information can be considered by the constraint of the princip information and the princip information that you may omit from the prospectua in an effective registration statement based on Rule 4304 (8.204.04.05 this chapter). The registrant must turnish this information in plain English. See § 230.421(d) of Regulation C of this chapter.	Functional	intersects with	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (ontional)	Notes (optional)
17 CFR 229.105(b)	N/A	Concisely explain how each risk effects the registrent or the securities being offered. If the discussion is longer than 15 pages, includes in the forepart of the prospectus or annual report, as applicable, a series of the properties of the prope	Functional	intersects with	Riak Register	RSK-04.1	Mechanisma exist to maintain a risk register that facilitates monitoring and reporting of risks. Mechanisma exist to define materiality threshold criteria capable of	5	
17 CFR 229.106(a)	N/A	Definitions. For purposes of this section: Cybersecurity incident means an unauthorized occurrence, or a series of related unauthorized occurrence, or or onducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein. Cybersecurity threat means any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information resources, owned or used by the registrant, information systems means electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or upport the registrant's operations.	Functional	intersects with	Materiality Determination	GOV-16	designating an incident as material.	5	
17 CFR 229.108(a)	N/A	Definitions. For purposes of this section: Cybersecurity incident means an unauthorized occurrence, or a series of related unauthorized occurrence, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of registrant's information systems or any information residing therein. Cybersecurity threat means any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information resident or setting therein. Information systems means electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.	Functional	intersects with	Material Threats	GOV-16.2	Mechanisms exist to define criteria necessary to designate a threat as a material threat.	5	
17 CFR 229.108(a)	N/A	osposition of the registrant's information to maintain or support the registrant's operations. Opheriscent, For purposes of this section: Ophersecutity incident means an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein. Ophersecutity threat means any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information esting therein. Information systems means electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant information to maintain or upport the registrant operations.	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, disription, modification or destruction of the organization's systems and data.	5	
17 CFR 229.108(a)	N/A	Definitions. For purposes of this section: Cybersecurity incident means an unauthorized occurrence, or a series of related unauthorized occurrence, on or conducted through a registrant's information systems that joepardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein. Cybersecurity threat means any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information systems and any or availability of a registrant's information residences, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or dissociation of the registrant's operations.	Functional	intersects with	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(t) and likelihood(s) of applicable internal and external threats.	5	
17 CFR 229.106(b)	N/A	Risk management and strategy. Describe the registrants processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In		no relationship	N/A Risk Management	N/A	N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.		No requirements to map to.
17 CFR 229.106(b)(1) 17 CFR 229.106(b)(1)	N/A N/A	providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items: Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:	Functional	subset of	Program Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring (2) Constraints affecting risk assessments, risk response and risk monitoring (3) The organizational risk tolerance; and (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for	5	
17 CFR 229.106(b)(1)	N/A	Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items.	Functional	intersects with	Risk Tolerance	RSK-01.3	manasine risk Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
17 CFR 229.106(b)(1)	N/A	Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:	Functional	intersects with	Risk Threshold	RSK-01.4	Mechanisms exist to define organizational risk threshold, the level of risk exposure above which risks are addressed and below which risks may be accepted.	5	
17 CFR 229.106(b)(1)	N/A	Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:	Functional	intersects with	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	5	
17 CFR 229.106(b)(1)	N/A	Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:	Functional	intersects with	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for systems, applications and/or services to prevent potential disruptions.	5	
17 CFR 229.106(b)(1)	N/A	Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items: Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external. Mechanisms exist to conduct recurring assessments of risk that includes	5	
17 CFR 229.106(b)(1)	N/A	Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from polyersecurity fivests in sufficient detail for a resonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure Items: Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unathroized access, use, disclosure, disruption, modification or destruction of the organization's systems and data. Mechanisms exist to identify and assign a risk ranking to newly discovered	5	
17 CFR 229.106(b)(1)	N/A	Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity fivests in sufficient featilit for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items: Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from	Functional	intersects with	Risk Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices. Mechanisms exist to remediate risks to an acceptable level.	5	
17 CFR 229.106(b)(1)	N/A	vescrive us registrants processes, it any, to assessing, behalfying, and inatisping interior insist from cybersecurity threats in sufficient fetal for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure Items: Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to respond to findings from cybersecurity & data privacy	5	
17 CFR 229.106(b)(1)	N/A	cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:	Functional	intersects with	Risk Response Operationalizing	RSK-06.1	assessments, incidents and audits to ensure proper remediation has been performed. Mechanisms exist to compel data and/or process owners to operationalize	5	
17 CFR 229.106(b)(1)(i)	N/A	Whether and how any such processes have been integrated into the registrant's overall risk management system or processes;	Functional	intersects with	Cybersecurity & Data Protection Practices	GOV-15	cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
17 CFR 229.106(b)(1)(i) 17 CFR 229.106(b)(1)(i)	N/A N/A	Whether and how any such processes have been integrated into the registrant's overall risk management system or processes: Whether and how any such processes have been integrated into the registrant's overall risk management system or processes;	Functional Functional	subset of intersects with	Risk Management Program Risk Framing	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tectical risk management controls. Mechanisms exist to identify: (I) Assumptions affecting risk assessments, risk response and risk monitoring. (2) Constraints affecting risk assessments, risk response and risk monitoring. (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-ofts considered by the organization for monastier risk.	5	



1985 1985	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)
March Marc	17 CFR 229.106(b)(1)(i)	N/A		Functional	intersects with	Risk Tolerance	RSK-01.3	range of acceptable results.	5	
March Marc	17 CFR 229.106(b)(1)(i)	N/A		Functional	intersects with	Risk Threshold	RSK-01.4	exposure above which risks are addressed and below which risks may be	5	
Page	17 CFR 229.106(b)(1)(i)	N/A		Functional	intersects with	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	5	
Column C	17 CFR 229.106(b)(1)(i)	N/A		Functional	intersects with	Risk Assessment	RSK-04	the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's	5	
1.	17 CFR 229.106(b)(1)(ii)	N/A		Functional	intersects with	& Data Protection	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection	5	
1.	17 CFR 229.106(b)(1)(ii)	N/A		Functional	intersects with	Requirements for Security-Related	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by	5	
March Marc	17 CFR 229.106(b)(1)(ii)	N/A		Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed	TPM-05.4	Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers	5	
Column C	17 CFR 229.106(b)(1)(iii)	N/A		Functional	intersects with	Management (SCRM)	RSK-09	(SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance	5	
March Marc	17 CFR 229.106(b)(1)(iii)	N/A		Functional	intersects with		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,	5	
Company Comp	17 CFR 229.106(b)(1)(iii)	N/A	associated with its use of any third-party service provider.	Functional	intersects with	Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
100-100-100-100-100-100-100-100-100-100			associated with its use of any third-party service provider.			Assessment		Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.		
1975 1976	17 CFR 229.106(b)(1)(iii)	N/A	associated with its use of any third-party service provider.	Functional	subset of		TPM-01	management controls. Mechanisms exist to identify, prioritize and assess suppliers and partners of	10	
	17 CFR 229.106(b)(1)(iii)	N/A	Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.	Functional	intersects with		TPM-02	assessment process relative to their importance in supporting the delivery of high-value services.	5	
Control 2015/000 Mail	17 CFR 229.106(b)(1)(iii)	N/A		Functional	intersects with		TPM-03	product supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
Part 20 10 10 10 10 10 10 10	17 CFR 229.106(b)(1)(iii)	N/A		Functional	intersects with		TPM-05	data privacy requirements with third-parties, reflecting the organization's	5	
Processed State Processed	17 CFR 229.106(b)(2)	N/A	cybersecurity incidents, have materially affected or are reasonably likely to materially affect the	Functional	subset of		GOV-16	Mechanisms exist to define materiality threshold criteria capable of	10	
1975-123-1000 NA	17 CFR 229.106(b)(2)	N/A	cybersecurity incidents, have materially affected or are reasonably likely to materially affect the	Functional	intersects with	Material Risks	GOV-16.1		5	
TOTA 25 100(01) No. 10 Control on the control of desiration of control on the control of control	17 CFR 229.106(b)(2)	N/A	cybersecurity incidents, have materially affected or are reasonably likely to materially affect the	Functional	intersects with	Material Threats	GOV-16.2		5	
TOTA 225-V00(0) NAL Control to be board of decision of the complete of the c	17 CFR 229.106(c)	N/A		Functional	no relationship		N/A	Mechanisms exist to coordinate cybersecurity, data protection and	N/A	No requirements to map to.
Description in No. Application of the comparison	17 CFR 229.106(c)(1)	N/A		Functional	subset of		GOV-01.1	comprised of key cybersecurity, data privacy and business executives,	10	
TOTR 221 106(CT) NA Secretary of the country of secretary when the country of th	17 CFR 229.106(c)(1)	N/A	board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and	Functional	intersects with		GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data	5	
Security of the contract of th	17 CFR 229.106(c)(1)	N/A	board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and	Functional	intersects with	& Data Protection	GOV-04	mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
17 CPR 226 109(012) NA Decide management's the in-assessing of managing the registration disable states and section the processes by the in-assessing of managing the registration disable states and between the communication of more analoging from individuals and teams related to management's table has been set or committee or described personal processing data and brothing against and the individual and teams and the i	17 CFR 229.106(c)(1)	N/A	board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and	Functional	intersects with		GOV-04.1	teams and individuals are empowered, responsible and trained for	5	
TOTR 223 109(c)(2) NA Whether and whether the registeries of experimental as a responsible for assessing and managing the forest season and the season and	17 CFR 229.106(c)(1)	N/A	board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and	Functional	intersects with		GOV-04.2	lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
17 CFR 229.109(c)[29] NA Whether and which management positions or committees are responsible for assessing and managing described the nature of the expertise. 10 miles and the committee of the prevention, described the nature of the expertise. 10 miles and the committee of the prevention of	17 CFR 229.106(c)(2)	N/A	cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:	Functional	intersects with		GOV-01.1	business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
Whether and which management positions or committees are responsible for assessing with management positions or committees are responsible for assessing and managing such risks, and the relevant expertises of the relative of the separtities. 17 CFR 229.109(2)(ii) NA Whether and which management positions or committees are responsible for assessing and managing such risks, and the remarkance propositions of committees are responsible for assessing and managing such risks, and the remarkance propositions of committees are responsible for assessing and managing such risks, and the remarkance propositions of committees are responsible for assessing and managing such risks, and the remarkance propositions of committees are responsible for assessing and managing such risks, and the remarkance propositions of committees are responsible for assessing and managing such risks, and the remarkance propositions of the separtition of committees or and separtition districts on the separtition of committees or and separation of separation of committees or and separation of the separation of committees or and separation of the separation of committees or and separation of the separation of committees or and separation of committees or and separation of committees or and separation of committees o	17 CFR 229.106(c)(2)	N/A	cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the	Functional	subset of		GOV-16		10	
Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant aspectation of such persons or members in such detail as necessary to fully discribe the nature of the expertise; 17 CFR 229.106(c)(2)(iii) N/A The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of opherescurity incidents; and committees or a formed about and monitor the prevention, detection, mitigation, and remediation of opherescurity incidents; and committee or subcommittee of the board of directors or a committee are prot information about such risks to the board of directors or a committee or subcommittee of the board of directors or a committee or subcommittee of the board of directors or a committee or subcommittee of the board of directors or a committee or subcommittee of the board of directors or a committee or subcommittee of the board of directors or a committee or subcommittee of the board of directors or a committee or subcommittee of the board of directors or a committee or subcommittee of the board of directors or a committee or subcommittee of the board of directors or a committee or subcommittee of the board of directors or a committee or subcommittee of the board of directors or a committee or subcommittee of the board of directors or a committee or subcommittee of the board of directors or a committee or subcommittee of the board of directors or a committee or subcommittee of the board of directors or a committee or subcommittee of the board of directors. 17 CFR 229.106(c)(7)(iii) N/A Villether such persons or committees are previously that is the internation about such risks to the board of directors or a committee or subcommittee of the board of directors. Functional To responsible that the previous of	17 CFR 229.106(c)(2)(i)	N/A	Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully	Functional	subset of		GOV-01.1	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	
To CFR 229.106(c)(2)(ii) N/A The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of operations; and detection, mitigation, and remediation of operations; and the committee of the board of directors or committee or subcommittee or the board of directors. To CFR 229.106(c)(2)(iii) N/A Whether such persons or committee or protinformation about such risks to the board of directors or committee or subcommittee of the board of directors. To CFR 229.106(c)(2)(iii) N/A Whether such persons or committees report information about such risks to the board of directors or committee or subcommittee of the board of directors. To CFR 229.106(c)(2)(iii) N/A Whether such persons or committee or subcommittee of directors. To CFR 229.106(c)(2)(iii) N/A Structured Data Requirement. Provide the information required by this item in an interactive Data File in succession with file 450 of Regulation 5-7 and the EDOAR file Menaus. Form B-K Item 1.05(ii) N/A Structured Data Requirement. Provide the information required by the registrant to be material, describe the material spects of the nature, scopes, and firming of the incident, and the material impact or reasonably likely material impact on the registrant for the material spects of the nature, scopes, and firming of the incident, and the material impact or reasonably likely material impact on the registrant, inciding its francial condition and results of correct with a describe the material spects of the nature, scopes, and firming of the incident, and the material impact or reasonably likely material impact on the registrant, inciding its francial condition and results or special conditions and the material impact or reasona	17 CFR 229.106(c)(2)(i)	N/A	such risks, and the relevant expertise of such persons or members in such detail as necessary to fully	Functional	intersects with	& Data Protection	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
Whether such persons or committees and persons or committee or subcommittee or	17 CFR 229.106(c)(2)(ii)	N/A		Functional	subset of		GOV-01.2	recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data orotection program.	10	
Whether such persons or committees any port information about such risks to the board of directors or committee or subcommittee or the board of directors or committee or subcommittee or the board of directors or committee or subcommittee or the board of directors or committee or subcommittee or subcommittee or the board of directors. 17 CFR 229.106(d) N/A Structured Dafa Requirement. Provide the information required by this Item in an interactive Dafa File in economic winds and the EDGAR Filer Menual. Form 8-K Item 1.05(a) N/A If the registrant experiences a cybersecurity incident that is determined by the registrant to be material support or reasonably likely material impact or the material sepacet of the mature, sepacet of the mature, sepacet of the mature, sepacet of the mature, sepacet of the material sepacet or reasonably likely material impact or the material sepacet of the mature, sepacet of the mature, sepacet of the mature, sepace, and thing of the registrant to be material impact or reasonably likely material impact or reasonably likely material impact or reasonably likely material impact	17 CFR 229.106(c)(2)(iii)	N/A		Functional	subset of		GOV-01.1	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	
17 CFR 229.106(d) N/A Structured butte requirement. Provide the information required by the refin and interactive bild a rie in authorized by the registrant to be material, specified or reasonably likely material impact or the material sepaction of the material	17 CFR 229.106(c)(2)(iii)	N/A		Functional	intersects with		GOV-01.2	recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
If the registrant experiences a cybensecurity incident that is determined by the registrant to be material, describe the material aspects of the mat	17 CFR 229.106(d)	N/A		Functional	subset of		GOV-17	cybersecurity and/or data privacy program to applicable statutory and/or	10	
From 8-K Item 1.05(a) Form 8-K Item 1.05(b) From	Form 8-K Item 1.05(a)	N/A	describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of	Functional	intersects with		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,	5	
If the registrant experiences a cybensecurity incident that is determined by the registrant to be material, describe the material aspect of the nature,	Form 8-K Item 1.05(a)	N/A	If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of	Functional	intersects with		GOV-16	Mechanisms exist to define materiality threshold criteria capable of	5	
If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, Form 8-K Item 1,05(a) N/A WA Mechanisms exist to implement and govern processes and documentation Incident Response Incident Re	Form 8-K Item 1.05(a)	N/A	If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of	Functional	intersects with		GOV-06		5	
operations.	Form 8-K Item 1.05(a)	N/A	If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of	Functional	intersects with		IRO-01	to facilitate an organization-wide response capability for cybersecurity &	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Form 8-K Item 1.05(a)	N/A	If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.	Functional	intersects with	Incident Handling		Mechanisms exist to cover: ((1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery	5	
Form 8-K Item 1.05(a)	N/A	If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.	Functional	intersects with	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5	
Form 8-K Item 1.05(a)	N/A	If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
Form 8-K Item 1.05(a)	N/A	If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.	Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
Form 8-K Item 1.05(a)	N/A	If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe the material spects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.	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.	5	
Form 8-K Item 1.05(a)	N/A	If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.	Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program	5	

