

**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:**

**SEC Cybersecurity Rule (2023)**

**Focal Document URL:** <https://www.sec.gov/files/rules/final/2023/33-11216.pdf>

**Published STRM URL:** <https://securecontrolsframework.com/content/strm/scf-strm-us-fed-sec-cybersecurity-rule.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) |
|-------------------|----------|--|----------------|-------------------|---|----------|--|-------------------------------------|------------------|
| 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 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   | Materiality Determination                     | GOV-16   | Mechanisms exist to define materiality 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 subcaption 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 "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 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 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 a subcaption 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     | 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 should be set forth under a subcaption 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 Framing                                  | RSK-01.1 | Mechanisms exist to identify:<br>(1) Assumptions affecting risk assessments, risk response and risk monitoring;<br>(2) Constraints affecting risk assessments, risk response and risk monitoring;<br>(3) The organizational risk tolerance; and<br>(4) Priorities, benefits and trade-offs considered by the organization for material risks                 | 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 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:<br>(1) Document the security categorization results (including supporting rationale) in the security plan for systems; and<br>(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 a subcaption 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 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 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      | Concise 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, bulleted 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 § 229.503 (Item 503 of Regulation S-K). If you do not include a summary section, the risk factor section must immediately follow the cover page of the prospectus or the pricing information section that immediately follows the cover page. Pricing information means price and price-related information that you may omit from the prospectus in an effective registration statement based on Rule 430A (§ 230.430A of this chapter). The registrant must furnish this information in plain English. See § 230.421(d) of Regulation C of this chapter. | 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      | Concise 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, bulleted 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 § 229.503 (Item 503 of Regulation S-K). If you do not include a summary section, the risk factor section must immediately follow the cover page of the prospectus or the pricing information section that immediately follows the cover page. Pricing information means price and price-related information that you may omit from the prospectus in an effective registration statement based on Rule 430A (§ 230.430A of this chapter). The registrant must furnish this information in plain English. See § 230.421(d) of Regulation C of this chapter. | 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      | Concise 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, bulleted 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 § 229.503 (Item 503 of Regulation S-K). If you do not include a summary section, the risk factor section must immediately follow the cover page of the prospectus or the pricing information section that immediately follows the cover page. Pricing information means price and price-related information that you may omit from the prospectus in an effective registration statement based on Rule 430A (§ 230.430A of this chapter). The registrant must furnish this information in plain English. See § 230.421(d) of Regulation C 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      | Concise 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, bulleted 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 § 229.503 (Item 503 of Regulation S-K). If you do not include a summary section, the risk factor section must immediately follow the cover page of the prospectus or the pricing information section that immediately follows the cover page. Pricing information means price and price-related information that you may omit from the prospectus in an effective registration statement based on Rule 430A (§ 230.430A of this chapter). The registrant must furnish this information in plain English. See § 230.421(d) of Regulation C of this chapter. | Functional     | subset of         | Cybersecurity & Data Privacy Status Reporting | GOV-17   | Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.  | 10                                  |                  |
| 17 CFR 229.105(b) | N/A      | Concise 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, bulleted 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 § 229.503 (Item 503 of Regulation S-K). If you do not include a summary section, the risk factor section must immediately follow the cover page of the prospectus or the pricing information section that immediately follows the cover page. Pricing information means price and price-related information that you may omit from the prospectus in an effective registration statement based on Rule 430A (§ 230.430A of this chapter). The registrant must furnish this information in plain English. See § 230.421(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 applicable laws, regulations and contractual obligations that:<br>(1) Document the security categorization results (including supporting rationale) in the security plan for systems; and<br>(2) Ensure the security categorization decision is reviewed and approved by the asset owner. | 5                                   |                  |
| 17 CFR 229.105(b) | N/A      | Concise 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, bulleted 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 § 229.503 (Item 503 of Regulation S-K). If you do not include a summary section, the risk factor section must immediately follow the cover page of the prospectus or the pricing information section that immediately follows the cover page. Pricing information means price and price-related information that you may omit from the prospectus in an effective registration statement based on Rule 430A (§ 230.430A of this chapter). The registrant must furnish 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 (optional) | Notes (optional)           |
|-------------------------|----------|--|----------------|-------------------|--|----------|---|-------------------------------------|----------------------------|
| 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 prospectus or annual report, as applicable, a series of concise, bulleted 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 § 229.503 (Item 503 of Regulation S-K). If you do not include a summary section, the risk factor section must immediately follow the cover page of the prospectus or the pricing information section that immediately follows the cover page. Pricing information means price and price-related information that you may omit from the prospectus in an effective registration statement based on Rule 430A (§ 230.430A of this chapter). The registrant must furnish this information in plain English. See § 230.421(d) of Regulation C of this chapter. | 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 229.106(a)       | N/A      | Definitions. For purposes of this section:<br><br>Cybersecurity 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.<br><br>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 or any information residing therein.<br><br>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   | Materiality Determination                                  | GOV-16   | Mechanisms exist to define materiality threshold criteria capable of designating an incident as material.   | 5                                   |                            |
| 17 CFR 229.106(a)       | N/A      | Definitions. For purposes of this section:<br><br>Cybersecurity 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.<br><br>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 or any information residing therein.<br><br>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 229.106(a)       | N/A      | Definitions. For purposes of this section:<br><br>Cybersecurity 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.<br><br>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 or any information residing therein.<br><br>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   | Risk Assessment  | RSK-04   | Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.  | 5                                   |                            |
| 17 CFR 229.106(a)       | N/A      | Definitions. For purposes of this section:<br><br>Cybersecurity 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.<br><br>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 or any information residing therein.<br><br>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   | Threat Analysis  | THR-10   | Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.  | 5                                   |                            |
| 17 CFR 229.106(b)       | N/A      | <b>Risk management and strategy.</b>   | Functional     | no relationship   | N/A  | N/A      | N/A   | N/A                                 | No requirements to map to. |
| 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     | subset of         | Risk Management Program                                    | RSK-01   | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.  | 10                                  |                            |
| 17 CFR 229.106(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 Framing   | RSK-01.1 | Mechanisms exist to identify:<br>(1) Assumptions affecting risk assessments, risk response and risk monitoring;<br>(2) Constraints affecting risk assessments, risk response and risk monitoring;<br>(3) The organizational risk tolerance; and<br>(4) Priorities, benefits and trade-offs considered by the organization for managing risk | 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 | 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:  | Functional     | Intersects with   | Risk Identification  | RSK-03   | Mechanisms exist to identify and document risks, both internal and external.  | 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 Assessment  | RSK-04   | Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.  | 5                                   |                            |
| 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 Ranking   | RSK-05   | Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.   | 5                                   |                            |
| 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 Remediation   | RSK-06   | Mechanisms exist to remediate risks to an acceptable level.   | 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 Response  | RSK-06.1 | Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.  | 5                                   |                            |
| 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   | Operationalizing Cybersecurity & Data Protection Practices | GOV-15   | Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.   | 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     | subset of         | Risk Management Program                                    | RSK-01   | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.  | 10                                  |                            |
| 17 CFR 229.106(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   | Risk Framing   | RSK-01.1 | Mechanisms exist to identify:<br>(1) Assumptions affecting risk assessments, risk response and risk monitoring;<br>(2) Constraints affecting risk assessments, risk response and risk monitoring;<br>(3) The organizational risk tolerance; and<br>(4) Priorities, benefits and trade-offs considered by the organization for managing risk | 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)           |
|---------------------------|----------|--|----------------|-------------------|--|----------|---|-------------------------------------|----------------------------|
| 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   | Risk Tolerance   | RSK-01.3 | Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.  | 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   | 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)(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   | 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)(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   | Risk Assessment  | RSK-04   | Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.  | 5                                   |                            |
| 17 CFR 229.106(b)(1)(ii)  | N/A      | Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and   | 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                                   |                            |
| 17 CFR 229.106(b)(1)(ii)  | N/A      | Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and   | Functional     | Intersects with   | Competency Requirements for Security-Related Positions                   | HRS-03.2 | Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.   | 5                                   |                            |
| 17 CFR 229.106(b)(1)(ii)  | N/A      | Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and   | Functional     | Intersects with   | Responsible, Accountable, Supportive, Consulted & Informed (RASC) Matrix | TPM-05.4 | Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).          | 5                                   |                            |
| 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   | Supply Chain Risk Management (SCRM) Plan                                 | RSK-09   | Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans. | 5                                   |                            |
| 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   | Steering Committee & Program Oversight                                   | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.   | 5                                   |                            |
| 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   | Status Reporting To Governing Body                                       | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.  | 5                                   |                            |
| 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   | Supply Chain Risk Assessment   | RSK-09.1 | Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.   | 5                                   |                            |
| 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     | subset of         | Third-Party Management   | TPM-01   | Mechanisms exist to facilitate the implementation of third-party management controls.   | 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   | Third-Party Criticality Assessments                                      | TPM-02   | Mechanisms exist to identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.  | 5                                   |                            |
| 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   | Supply Chain Risk Management (SCRM)                                      | TPM-03   | Mechanisms exist to: (1) Evaluate security risks and threats associated with the services and product supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.   | 5                                   |                            |
| 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   | Third-Party Contract Requirements  | TPM-05   | Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.  | 5                                   |                            |
| 17 CFR 229.106(b)(2)      | N/A      | Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how.                              | Functional     | subset of         | Materiality Determination  | GOV-16   | Mechanisms exist to define materiality threshold criteria capable of designating an incident as material.   | 10                                  |                            |
| 17 CFR 229.106(b)(2)      | N/A      | Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how.                              | 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 229.106(b)(2)      | N/A      | Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how.                              | 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 229.106(c)         | N/A      | Governance   | Functional     | no relationship   | N/A  | N/A      | N/A   | N/A                                 | No requirements to map to. |
| 17 CFR 229.106(c)(1)      | N/A      | Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.                              | 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                                  |                            |
| 17 CFR 229.106(c)(1)      | N/A      | Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.                              | Functional     | Intersects with   | Status Reporting To Governing Body                                       | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.  | 5                                   |                            |
| 17 CFR 229.106(c)(1)      | N/A      | Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.                              | 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                                   |                            |
| 17 CFR 229.106(c)(1)      | N/A      | Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.                              | Functional     | Intersects with   | Stakeholder Accountability Structure                                     | GOV-04.1 | Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.   | 5                                   |                            |
| 17 CFR 229.106(c)(1)      | N/A      | Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.                              | Functional     | Intersects with   | Authoritative Chain of Command   | GOV-04.2 | Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.   | 5                                   |                            |
| 17 CFR 229.106(c)(2)      | N/A      | Describe management's role in assessing and managing the registrant's material risks from cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:   | Functional     | Intersects with   | Steering Committee & Program Oversight                                   | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.   | 5                                   |                            |
| 17 CFR 229.106(c)(2)      | N/A      | Describe management's role in assessing and managing the registrant's material risks from cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:   | Functional     | subset of         | Materiality Determination  | GOV-16   | Mechanisms exist to define materiality threshold criteria capable of designating an incident as material.   | 10                                  |                            |
| 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 describe the nature of the expertise;   | 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                                  |                            |
| 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 describe the nature of the expertise;   | 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                                   |                            |
| 17 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 cybersecurity incidents; and  | Functional     | subset of         | Status Reporting To Governing Body                                       | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.  | 10                                  |                            |
| 17 CFR 229.106(c)(2)(iii) | N/A      | Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.   | 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                                  |                            |
| 17 CFR 229.106(c)(2)(iii) | N/A      | Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.   | Functional     | Intersects with   | Status Reporting To Governing Body                                       | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.  | 5                                   |                            |
| 17 CFR 229.106(d)         | N/A      | Structured Data Requirement. Provide the information required by this item in an Interactive Data File in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual.   | Functional     | subset of         | Cybersecurity & Data Privacy Status Reporting                            | GOV-17   | Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.   | 10                                  |                            |
| 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   | Steering Committee & Program Oversight                                   | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.   | 5                                   |                            |
| 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   | Materiality Determination  | GOV-16   | Mechanisms exist to define materiality threshold criteria capable of designating an incident as material.   | 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   | Contacts With Authorities  | GOV-06   | Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.   | 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 Operations   | IRO-01   | Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.   | 5                                   |                            |

| 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   | IRO-02   | Mechanisms exist to cover:<br>(1) Preparation;<br>(2) Automated event detection or manual incident report intake;<br>(3) Analysis;<br>(4) Containment;<br>(5) Eradication; and<br>(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 (RP) 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 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 Stakeholder Reporting                            | IRO-10   | Mechanisms exist to timely-report incidents to applicable:<br>(1) Internal stakeholders;<br>(2) Affected clients & third-parties; and<br>(3) Regulatory authorities.   | 5                                   |                  |
| Form 8-K Item 1.05(a)(i) | 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                                   |                  |