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

Focal Document: Nevada Operation of Gaming Establishments - Regulation 5.260 (Cybersecurity)
Focal Document URL: https://www.gaming.nv.gov/siteassets/content/home/features/regulationSoperation.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-nv-regulation-5-2024.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
5.260.1	N/A	In accordance with the public policy of the State set forth in NRS 463.0129 and the requirements set forth in chapter 603A of NRS, it is critical that gaming operators take all appropriate steps to secure and protect their information systems from the ongoing threat of cyber attacks. Gaming operators must not only secure and protect their own records and operations, but also the personal information of their patrons and employees as defined in NRS 603A.040.	Functional	Subset of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
5.260.1	N/A	In accordance with the public policy of the State set forth in NRS 463.0129 and the requirements set forth in chapter 603A of NRS, it is critical that gaming operators take all appropriate steps to secure and protect their information systems from the ongoing threat of cyber attacks. Gaming operators must not only secure and protect their own records and operations, but also the personal information of their patrons and employees as defined in NRS 603A.040.	Functional	Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	8	
5.260.1	N/A	In accordance with the public policy of the State set forth in NRS 463.0129 and the requirements set forth in chapter 603A of NRS, it is critical that gaming operators take all appropriate steps to secure and protect their information systems from the ongoing threat of cyber attacks. Gaming operators must not only secure and protect their own records and operations, but also the personal information of their patrons and employees as defined in NRS 603A.040.	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	8	
5.260.2	N/A	Definitions. As used in this section: (a) "Cyber attack" means any act or attempt to gain unauthorized access to an information system for purpose of disrupting, disabling, destroying, or controlling the system or destroying or gaining access to the information contained therein. (b) "Cybersecurity" means the process of protecting an information system by preventing, detecting, and responding to cyber attacks. (c) "Covered entity" means an entity required to comply with the requirements of this section. Each of the following qualify as a covered entity: (1) Holder of a nonrestricted license as defined in NRS 463.0177 who deals, operates, carries on, conducts, maintains, or exposes for play any game defined in NRS 463.0152; (2) Holder of a gaming license that allows for the operation of a race book; (3) Holder of a gaming license that allows for the operation of a sports pool; and (4) Holder of a gaming license that permits the operation of interactive gaming. (d) "Information system" means a set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Elements of an information system include, without limit, hardware, software, information, data, applications, communications, and people. (e) "Risk assessment" means the process of identifying, estimating, and prioritizing risks to organizational operations and assets resulting from the operation of an information system. Guidance for conducting a risk assessment can be found in the Framework for Improving Critical Infrastructure Cybersecurity, version 1.1 or later, published by NIST.	Functional	Subset of	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	10	
5.260.3	N/A	Except as otherwise provided herein, a covered entity shall perform an initial risk assessment of its business operation and develop the cybersecurity best practices it deems appropriate. After performing the initial risk assessment, the covered entity shall continue to monitor and evaluate cybersecurity risks to its business operation on an ongoing basis and shall modify its cybersecurity best practices and risk assessments as it deems appropriate. The risk assessment and ongoing monitoring and evaluation required pursuant to this subsection may be performed by an affiliate of the covered entity or a third-party with expertise in the field of cybersecurity. Examples of cybersecurity best practices include, without limit, CIS Version 8, COBIT 5, ISO/IEC 27001, and NIST SP 800-53, or later versions thereof. Covered entities shall fully comply with this subsection within 90 days of being licensed.	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	5	
5.260.3	N/A	Except as otherwise provided herein, a covered entity shall perform an initial risk assessment of its business operation and develop the cybersecurity best practices it deems appropriate. After performing the initial risk assessment, the covered entity shall continue to monitor and evaluate cybersecurity risks to its business operation on an ongoing basis and shall modify its cybersecurity best practices and risk assessments as it deems appropriate. The risk assessment and ongoing monitoring and evaluation required pursuant to this subsection may be performed by an affiliate of the covered entity or a third-party with expertise in the field of cybersecurity. Examples of cybersecurity best practices include, without limit, CIS Version 8, COBIT 5, ISO/IEC 27001, and NIST SP 800-53, or later versions thereof. Covered entities shall fully comply with this subsection within 90 days of being licensed.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
5.260.3	N/A	Except as otherwise provided herein, a covered entity shall perform an initial risk assessment of its business operation and develop the cybersecurity best practices it deems appropriate. After performing the initial risk assessment, the covered entity shall continue to monitor and evaluate cybersecurity risks to its business operation on an ongoing basis and shall modify its cybersecurity best practices and risk assessments as it deems appropriate. The risk assessment and ongoing monitoring and evaluation required pursuant to this subsection may be performed by an affiliate of the covered entity or a third-party with expertise in the field of cybersecurity. Examples of cybersecurity best practices include, without limit, CIS Version 8, COBIT 5, ISO/IEC 27001, and NIST SP 800-53, or later versions thereof. Covered entities shall fully comply with this subsection within 90 days of being licensed.	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
5.260.3	N/A	Except as otherwise provided herein, a covered entity shall perform an initial risk assessment of its business operation and develop the cybersecurity best practices it deems appropriate. After performing the initial risk assessment, the covered entity shall continue to monitor and evaluate cybersecurity risks to its business operation on an ongoing basis and shall modify its cybersecurity best practices and risk assessments as it deems appropriate. The risk assessment and ongoing monitoring and evaluation required pursuant to this subsection may be performed by an affiliate of the covered entity or a third-party with expertise in the field of cybersecurity. Examples of cybersecurity best practices include, without limit, CIS Version 8, COBIT 5, ISO/IEC 27001, and NIST SP 800-53, or later versions thereof. Covered entities shall fully comply with this subsection within 90 days of being licensed.	Functional	Intersects With	Risk Assessment Update	RSK-07	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	8	
5.260.4	N/A	A covered entity that experiences a cyber attack to its information system resulting in a material loss of control, compromise, unauthorized disclosure of data or information, or any other similar occurrence shall:	Functional	Intersects With	Materiality Determination	GOV-16	Mechanisms exist to define materiality threshold criteria capable of designating an incident as material.	5	
5.260.4(a)	N/A	Provide written notification of the cyber attack to the Board as soon as practicable but no later than 72 hours after becoming aware of the cyber attack. Upon request, the covered entity shall provide the Board with specific information regarding the cyber attack;	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	8	
5.260.4(b)	N/A	Perform, or have a third-party perform, an investigation into the cyber attack, prepare a report documenting the results of the investigation, notify the Board of the completion of the report, and make the report available to the Board for review upon request. The report must include, without limit, the root cause of the cyber attack, the extent of the cyber attack, and any actions taken or planned to be taken to prevent similar events that allowed the cyber attack to occur; and	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 Security, Compliance & Resilience Program (SCRP).	8	
5.260.4(b)	N/A	Perform, or have a third-party perform, an investigation into the cyber attack, prepare a report documenting the results of the investigation, notify the Board of the completion of the report, and make the report available to the Board for review upon request. The report must include, without limit, the root cause of the cyber attack, the extent of the cyber attack, and any actions taken or planned to be taken to prevent similar events that allowed the cyber attack to occur; and	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	8	
5.260.4(c)	N/A	Notify the Board when any investigation or similar action taken by an entity external to the covered entity is completed and make the results of such investigation or similar action available to the Board upon request.	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 Security, Compliance & Resilience Program (SCRP).	8	
5.260.4(c)	N/A	Notify the Board when any investigation or similar action taken by an entity external to the covered entity is completed and make the results of such investigation or similar action available to the Board upon request.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	8	
5.260.5	N/A	A covered entity that has been classified as a Group I licensee as defined in subsection 8 of regulation 6.010 shall:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
5.260.5(a)	N/A	Designate a qualified individual to be responsible for developing, implementing, overseeing, and enforcing the covered entity's cybersecurity best practices and procedures developed pursuant to subsection 3.	Functional	Equal	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	10	
5.260.5(b)	N/A	At least annually, have its internal auditor or other independent entity with expertise in the field of cybersecurity perform and document observations, examinations, and inquiries of employees to verify the covered entity is following the cybersecurity best practices and procedures developed pursuant to subsection 3. A covered entity shall retain all documents prepared by the internal auditor pursuant to this paragraph in accordance with the requirements set forth in subsection 6. The same independent entity utilized under this paragraph may be utilized to perform the procedures set forth in paragraph (c) provided the procedures in this paragraph are performed by different employees.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	8	
5.260.5(b)	N/A	At least annually, have its internal auditor or other independent entity with expertise in the field of cybersecurity perform and document observations, examinations, and inquiries of employees to verify the covered entity is following the cybersecurity best practices and procedures developed pursuant to subsection 3. A covered entity shall retain all documents prepared by the internal auditor pursuant to this paragraph in accordance with the requirements set forth in subsection 6. The same independent entity utilized under this paragraph may be utilized to perform the procedures set forth in paragraph (c) provided the procedures in this paragraph are performed by different employees.	Functional	Intersects With	Periodic Audits	CPL-02.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	8	
5.260.5(b)	N/A	At least annually, have its internal auditor or other independent entity with expertise in the field of cybersecurity perform and document observations, examinations, and inquiries of employees to verify the covered entity is following the cybersecurity best practices and procedures developed pursuant to subsection 3. A covered entity shall retain all documents prepared by the internal auditor pursuant to this paragraph in accordance with the requirements set forth in subsection 6. The same independent entity utilized under this paragraph may be utilized to perform the procedures set forth in paragraph (c) provided the procedures in this paragraph are performed by different employees.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
5.260.5(c)	N/A	At least annually, engage an independent accountant or other independent entity with expertise in the field of cybersecurity to perform an independent review of the covered entity's best practices and procedures developed pursuant to subsection 3 and attest in writing that those practices and procedures comply with the requirements of this section. The covered entity shall retain the written attestation, and any related documents provided therewith, in accordance with the requirements set forth in subsection 6. The same independent entity utilized under this paragraph may be utilized to perform the procedures set forth in paragraph (b) provided the procedures in this paragraph are performed by different employees.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
5.260.5(c)	N/A	At least annually, engage an independent accountant or other independent entity with expertise in the field of cybersecurity to perform an independent review of the covered entity's best practices and procedures developed pursuant to subsection 3 and attest in writing that those practices and procedures comply with the requirements of this section. The covered entity shall retain the written attestation, and any related documents provided therewith, in accordance with the requirements set forth in subsection 6. The same independent entity utilized under this paragraph may be utilized to perform the procedures set forth in paragraph (b) provided the procedures in this paragraph are performed by different employees.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
5.260.5(c)	N/A	At least annually, engage an independent accountant or other independent entity with expertise in the field of cybersecurity to perform an independent review of the covered entity's best practices and procedures developed pursuant to subsection 3 and attest in writing that those practices and procedures comply with the requirements of this section. The covered entity shall retain the written attestation, and any related documents provided therewith, in accordance with the requirements set forth in subsection 6. The same independent entity utilized under this paragraph may be utilized to perform the procedures set forth in paragraph (b) provided the procedures in this paragraph are performed by different employees.	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-05.8	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	8	
5.260.6	N/A	A covered entity shall document in writing all procedures taken to comply with this section and the results thereof. The covered entity shall retain all records required in this section for a minimum of five years from the date they are created unless the Chair approves otherwise in writing. The covered entity shall provide any record required in this section to the Board upon request.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
5.260.6	N/A	A covered entity shall document in writing all procedures taken to comply with this section and the results thereof. The covered entity shall retain all records required in this section for a minimum of five years from the date they are created unless the Chair approves otherwise in writing. The covered entity shall provide any record required in this section to the Board upon request.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
5.260.7	N/A	Failure to exercise proper due diligence in compliance with this section shall constitute an unsuitable method of operation and may result in disciplinary action. (Adopted: 12/22. Amended: 7/24.)	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	

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

Focal Document: Nevada Operation of Gaming Establishments - Regulation 5.260 (Cybersecurity)
Focal Document URL: https://www.gaming.nv.gov/siteassets/content/home/features/regulation5operation.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-nv-regulation-5-2024.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
5.260.1	N/A	In accordance with the public policy of the State set forth in NRS 463.0129 and the requirements set forth in chapter 603A of NRS, it is critical that gaming operators take all appropriate steps to secure and protect their information systems from the ongoing threat of cyber attacks. Gaming operators must not only secure and protect their own records and operations, but also the personal information of their patrons and employees as defined in NRS 603A.040.	Functional	Subset Of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
				Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	8	
				Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	8	
5.260.2	N/A	Definitions. As used in this section: (a) "Cyber attack" means any act or attempt to gain unauthorized access to an information system for purpose of disrupting, disabling, destroying, or controlling the system or destroying or gaining access to the information contained therein. (b) "Cybersecurity" means the process of protecting an information system by preventing, detecting, and responding to cyber attacks. (c) "Covered entity" means an entity required to comply with the requirements of this section. Each of the following qualify as a covered entity: (1) Holder of a nonrestricted license as defined in NRS 463.0177 who deals, operates, carries on, conducts, maintains, or exposes for play any game defined in NRS 463.0152; (2) Holder of a gaming license that allows for the operation of a race book; (3) Holder of a gaming license that allows for the operation of a sports pool; and (4) Holder of a gaming license that permits the operation of interactive gaming. (d) "Information system" means a set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Elements of an information system include, without limit, hardware, software, information, data, applications, communications, and people. (e) "Risk assessment" means the process of identifying, estimating, and prioritizing risks to organizational operations and assets resulting from the operation of an information system. Guidance for conducting a risk assessment can be found in the Framework for Improving Critical Infrastructure Cybersecurity, version 1.1 or later, published by NIST.	Functional	Subset Of	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	10	
5.260.3	N/A	Except as otherwise provided herein, a covered entity shall perform an initial risk assessment of its business operation and develop the cybersecurity best practices it deems appropriate. After performing the initial risk assessment, the covered entity shall continue to monitor and evaluate cybersecurity risks to its business operation on an ongoing basis and shall modify its cybersecurity best practices and risk assessments as it deems appropriate. The risk assessment and ongoing monitoring and evaluation required pursuant to this subsection may be performed by an affiliate of the covered entity or a third-party with expertise in the field of cybersecurity. Examples of cybersecurity best practices include, without limit, CIS Version 8, COBIT 5, ISO/IEC 27001, and NIST SP 800-53, or later versions thereof. Covered entities shall fully comply with this subsection within 90 days of being licensed.	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate cybersecurity and data protection controls at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	5	
				Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
				Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
				Intersects With	Risk Assessment Update	RSK-07	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	8	
5.260.4	N/A	A covered entity that experiences a cyber attack to its information system resulting in a material loss of control, compromise, unauthorized disclosure of data or information, or any other similar occurrence shall:	Functional	Intersects With	Materiality Determination	GOV-16	Mechanisms exist to define materiality threshold criteria capable of designating an incident as material.	5	
5.260.4(a)	N/A	Provide written notification of the cyber attack to the Board as soon as practicable but no later than 72 hours after becoming aware of the cyber attack. Upon request, the covered entity shall provide the Board with specific information regarding the cyber attack;	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	8	
5.260.4(b)	N/A	Perform, or have a third-party perform, an investigation into the cyber attack, prepare a report documenting the results of the investigation, notify the Board of the completion of the report, and make the report available to the Board for review upon request. The report must include, without limit, the root cause of the cyber attack, the extent of the cyber attack, and any actions taken or planned to be taken to prevent similar events that allowed the cyber attack to occur; and	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 and data protection program.	8	
				Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	8	
5.260.4(c)	N/A	Notify the Board when any investigation or similar action taken by an entity external to the covered entity is completed and make the results of such investigation or similar action available to the Board upon request.	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 and data protection program.	8	
				Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	8	
5.260.5	N/A	A covered entity that has been classified as a Group I licensee as defined in subsection 8 of regulation 6.010 shall:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.260.5(a)	N/A	Designate a qualified individual to be responsible for developing, implementing, overseeing, and enforcing the covered entity's cybersecurity best practices and procedures developed pursuant to subsection 3.	Functional	Equal	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program.	10	
5.260.5(b)	N/A	At least annually, have its internal auditor or other independent entity with expertise in the field of cybersecurity perform and document observations, examinations, and inquiries of employees to verify the covered entity is following the cybersecurity best practices and procedures developed pursuant to subsection 3. A covered entity shall retain all documents prepared by the internal auditor pursuant to this paragraph in accordance with the requirements set forth in subsection 6. The same independent entity utilized under this paragraph may be utilized to perform the procedures set forth in paragraph (c) provided the procedures in this paragraph are performed by different employees.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	8	
				Intersects With	Periodic Audits	CPL-02.2	Mechanisms exist to conduct periodic audits of cybersecurity and data protection controls to evaluate conformity with the organization's documented policies, standards and procedures.	8	
				Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
5.260.5(c)	N/A	At least annually, engage an independent accountant or other independent entity with expertise in the field of cybersecurity to perform an independent review of the covered entity's best practices and procedures developed pursuant to subsection 3 and attest in writing that those practices and procedures comply with the requirements of this section. The covered entity shall retain the written attestation, and any related documents provided therewith, in accordance with the requirements set forth in subsection 6. The same independent entity utilized under this paragraph may be utilized to perform the procedures set forth in paragraph (b) provided the procedures in this paragraph are performed by different employees.	Functional	Intersects With	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements.	5	
				Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
				Intersects With	Third-Party Attestation (3PA)	TPM-05.8	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to contractors and subcontractors.	8	
5.260.6	N/A	A covered entity shall document in writing all procedures taken to comply with this section and the results thereof. The covered entity shall retain all records required in this section for a minimum of five years from the date they are created unless the Chair approves otherwise in writing. The covered entity shall provide any record required in this section to the Board upon request.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	
				Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
5.260.7	N/A	Failure to exercise proper due diligence in compliance with this section shall constitute an unsuitable method of operation and may result in disciplinary action. (Adopted: 12/22. Amended: 7/24.)	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control